H-**Diplo** | **ISSF** Roundtable XII-9

issforum.org

Jon R. Lindsay. ***Information Technology and Military Power.*** Ithaca: Cornell University Press, 2020. ISBN: 9781501749568 (hardcover, $42.95).

26 April 2021 | https://issforum.org/to/ir-12-9
Editor: Diane Labrosse | Commissioning Editor: Rebecca Slayton | Production Editor: George Fujii

Contents

Introduction by Ryan Grauer, University of Pittsburgh

War is a complex and chaotic business that persistently confounds the attempts of frontline forces, junior officers, field commanders, campaign commanders, policy elites, and others to understand what is happening amidst the smoke, noise, violence, and confusion. This has not, however, stopped war's many participants from trying to discern the ebbs and flows of battle and use whatever information can be gleaned to chart the most propitious path forward. Information technology has always been a central component of this effort; as the Chief of the Prussian General Staff, Helmuth von Moltke, noted soon after the employment of the telegraph in battle, the goal of reliance on tools ranging from human and animal messengers to the most sophisticated, integrated satellite-based communications networks has been to improve a military's ability to estimate and respond to the current and likely future combat situation.[1]

In *Information Technology and Military Power*, Jon R. Lindsay explains why, despite millennia of innovation and development in information technologies (including the bewildering array of advances achieved in the past few decades) and repeated forecasts of wartime omniscience lying just over the horizon, militaries still struggle to "lift the fog of war."[2] The answer, he argues, lies in the fact that information technology is used by the human-populated organizations that fight wars. "Information practice," or the way in which military organizations handle, interpret, and exploit information gathered and transmitted by various technologies as they navigate the trials of combat, can vary in its quality depending on the extent to which the external problems the armed forces confront are structured and the internal solutions to those problems are institutionalized (7). Performance in war, he suggests, will generally follow performance in information practice. Lindsay demonstrates the analytical utility of his claim through four exceptionally detailed case studies, two of which are derived in part from ethnographic work he carried out while deployed during the Kosovo and Iraq wars.

The result of Lindsay's efforts, the contributors to this roundtable unanimously conclude, is a remarkable book that builds on and contributes to a wide range of literatures, ranging from international relations and military effectiveness to information science and organization theory. Stephen Biddle notes that the argument is "persuasive and important," and that Lindsay's case studies "evoke a sense of place" rarely seen in academic works. Audrey Kurth Cronin concurs, stating that the book offers "shrewd analysis" and "invaluable evidence," and should be read by a wide range of scholars and practitioners. Myriam Dunn Cavelty writes that, among the "many great things" about Lindsay's book are its "theoretically innovative take on the challenges of digital transformation in the public sector" and empirical richness supplemented with "an at times charmingly auto-ethnographic account of experiencing information friction while serving in the U.S. military." Paul N. Edwards goes so far as to declare *Information Technology and Military Power* "a masterpiece."

The uniform praise of Lindsay's book (to which I would add my own voice) is telling given the disciplinary diversity of this exceptionally qualified group of reviewers. Biddle, a professor of international and public affairs at Columbia University, is perhaps unique in his academic expertise and familiarity with modern military operations, the latter earned in no small part through countless hours spent among operational units (including in Iraq). Cronin, a professor of international security at American University, is a leading expert on the intersection of emerging technologies and political violence, particularly with respect to terrorism and counterterrorism. Dunn Cavelty, a senior lecturer for security studies at ETH Zürich, researches and advises a range of public and private actors around the world on cyber security, cyber warfare, and risk analysis. Edwards is professor (emeritus) of information history at the University of Michigan and currently directs the Program on Science, Technology, and Society at Stanford University. That these accomplished scholars working in such disparate fields all agree on the merits of Lindsay's book is in itself a powerful comment on its quality.

[1] Helmuth Karl Bernard von Moltke, *Moltke On the Art of War: Selected Writings*, ed. Daniel J. Hughes, trans. Daniel J. Hughes and Harry Bell (New York: Ballantine Books, 1993), 113.

[2] William A. Owens, *Lifting the Fog of War* (Baltimore: The Johns Hopkins University Press, 2001).

While effusive in their commendation, the contributors to this roundtable do offer some critiques Lindsay's argument. The full reviews merit reading, as does Lindsay's thoughtful response, but a few of the criticisms are worth highlighting in this brief introduction. First, Cronin suggests that Lindsay's invocation of the "technology theory of victory," and particularly the Revolution in Military Affairs (RMA), as a foil occasionally seems to refer to a slightly overwrought paper tiger of an idea to which few dogmatically adhere; a more grounded engagement with the specific ideas of militaries, she suggests, would have strengthened his claim. Dunn Cavelty is less concerned by Lindsay's "passionate plea against letting technological determinism as manifest in the 'technology theory of victory' guide our thinking about military power," but does question the extent to which the model articulated in the book adequately captures the complex interrelation between military organizations, the information they collect and analyze, and the environments within which they act. Information practices, Dunn Cavelty notes, not only reveal the environment, but can transform (and, in some cases, construct) it. All theories necessitate some abstraction from reality, but how much abstraction is permissible before theory ceases to provide analytical leverage on the phenomena under investigation?

Perhaps the most strident criticism of Lindsay's work is levied by Biddle and Dunn Cavelty, and it concerns his case selection. Lindsay examines British information practice during the Battle of Britain and American information practices with respect to the development of the FalconView mapping system that is used for flight mission planning, special forces' conduct of counterinsurgent operations in Iraq, and the use of remotely piloted aircraft (drones) in counterterrorism operations. Both Biddle and Dunn Cavelty note that the logic for selecting the cases is not especially clear unless one consults the methodological appendix to the main text and, even then, readers are left uncertain as to whether they have much scientific utility beyond illustration. Biddle adds that, rich as they are, the cases do not always provide a clear link between information practice and the overarching concept on which Lindsay seeks to shed light (and even includes in his title): military power. Lindsay explicitly notes in the methodological appendix that his project is one of conjecture rather than refutation (243), but the criticism is an important one: clarity on how well and how far his argument travels will not only help scholars understand variations in military power, but also judge the merits of the compelling organizational reform recommendations made in the concluding chapter of the book.

Ultimately, the contributors to the roundtable judge that the merits of Lindsay's work considerably outweigh its shortcomings. They all note new questions and ideas raised by *Information Technology and Military Power* that warrant further investigation, whether by Lindsay or the many scholars who will undoubtedly follow in his footsteps. In many ways, the noting of those questions and ideas is the highest praise a book might receive; by combining insights from multiple disciplines and applying them to a vitally important contemporary problem, Lindsay has shown that there is much that scholars and practitioners have yet to learn about how information technology and practice drives organizational performance, and that the learning will be worthwhile.

Participants:

Jon Lindsay is Assistant Professor of Digital Media and Global Affairs at the Munk School of Global Affairs and Public Policy and in the Department of Political Science at the University of Toronto. He is the author of *Information Technology and Military Power* (Cornell, 2020) and co-editor of *Cross-Domain Deterrence* (Oxford, 2019) and *China and Cybersecurity* (Oxford, 2015).

Ryan Grauer is an Associate Professor of International Affairs in the Graduate School of Public and International Affairs at the University of Pittsburgh. His research examines the sources and use of military power in the international arena; the creation, organization, and operation of multinational coalitions in battle; and the causes and consequences of soldier surrender in war. He is the author of *Commanding Military Power* (Cambridge University Press, 2016).

Stephen Biddle is Professor of International and Public Affairs at Columbia University, and Adjunct Senior Fellow for Defense Policy at the Council on Foreign Relations. His research focuses on U.S. defense policy, international security, the conduct of war, military technology, and the analysis of recent combat operations. He has served on the Defense Policy Board, and as a member of theater assessment teams under Generals David Petraeus and Lloyd Austin in Iraq and General

Stanley McChrystal in Afghanistan. He has held teaching and research positions at the Council on Foreign Relations, George Washington University, the U.S. Army War College, the University of North Carolina, and the Institute for Defense Analyses.

Audrey Kurth Cronin is Professor of International Security at American University in Washington, DC. She is widely published on strategy and nonstate actors. Her best-known book is *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns* (Princeton University Press, 2009), recently translated into Chinese. In 2017*, The New Yorker* called it a "landmark study." Her latest book, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2020), analyzes the risks and opportunities of new or emerging technologies, including drones (UAVs), robotics, the Internet of Things, autonomy, and artificial intelligence, especially their use by terrorists, insurgents and other private actors. She regularly advises at senior levels of the U.S. government and has led or co-led field studies in Algeria, Morocco, Tunisia, Turkey, Saudi Arabia, India, Pakistan, Mexico, and Colombia. She has also been Chairman of the World Economic Forum's Global Agenda Council on Terrorism and is a life member of the Council on Foreign Relations.

Myriam Dunn Cavelty is senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS) at ETH Zürich, Switzerland. She is the author of several books, edited volumes and journal articles on cyber security politics, including *Cyber-Security and Threat Politics* (Routledge, 2008).

Paul N. Edwards is Director of the Program on Science, Technology & Society at Stanford University and Professor of Information and History (Emeritus) at the University of Michigan. He writes and teaches about the history, politics, and culture of knowledge infrastructures. Edwards is the author of *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming* (MIT Press, 2010) and *The Closed World: Computers and the Politics of Discourse in Cold War America* (MIT Press, 1996), and co-editor of *Changing the Atmosphere: Expert Knowledge and Environmental Governance* (MIT Press, 2001), as well as numerous articles. With Geoffrey Bowker, he co-edits a book series, *Infrastructures*, for MIT Press.

Review by Stephen Biddle, Columbia University

In *Information Technology and Military Power*, Jon Lindsay argues that hardware and software explain only part of what matters in information-age warfare. The wetware – that is, the human beings behind the equipment, and the organizations and procedures that shape those humans' behavior – matters at least as much. He makes this case via a detailed deductive argument and four in-depth case studies of military organizations' use of information technology: the Royal Air Force's use of radar in the Battle of Britain in 1940-41; the U.S. Air Force's use of mission planning software in the 1990s-2000s; U.S. Special Operations Forces' use of a suite of networked information technology for counterinsurgency in Iraq's Anbar Province in 2007; and the U.S. use of drones for reconnaissance and leadership targeting after 2001. The result is a compelling account of an increasingly important issue.

Lindsay's deductive theory explains an organization's "information practice" (2) by reference to two chief explanatory variables, each of which has two potential states: the organization's "external problem" (which can be *constrained* or *unconstrained*) and its "internal solution" for addressing that problem (which can be *institutionalized* or *organic*). This yields the inescapable political science 2x2 table of outcomes. When *constrained* external problems are met with *institutionalized* internal solutions, the result is "managed practice" (57-59), the best-case outcome. Enemies facing this have an incentive to change their behavior to create ambiguity and misperception; this often shifts the external problem to one that is *unconstrained*. If one's internal solution remains *institutionalized* in the face of this change, the result is "insulated practice," (59-62) in which the routinized procedures of "managed practice" (57-59) become ill-adapted to a more complex threat environment and perception becomes increasingly divorced ("insulated" 59-62) from the new realities of the battlespace. Bruising experiences of insulation against an *unconstrained* external problem encourage a shift from an institutionalized to an *organic* internal solution. This combination yields a more satisfactory outcome of "adaptive practice" (62-65), in which less routinized information behavior yields a higher rate of helpful innovation, enabling an improvement in the fit between perception and battlespace reality.

But this in turn encourages the enemy to regularize its own tactics around the best practices that emerge from a period of unconstrained behavior; the resulting combination of a now-*constrained* external problem with a still-*organic* internal solution yields the unsatisfactory outcome of "problematic practice" (65-67), in which over-innovation by information practitioners yields change that is bad as often as good. The resulting mismatch between perception and reality then encourages a shift from an organic back to an *institutionalized* internal solution to this *constrained* external problem, bringing us back to the "managed practice" outcome where we began, with the more satisfactory results this cell in the table produces. The result is a tendency for information practice to cycle among the four cells of the 2x2, from managed to insulated to adaptive to problematic practice, and back to managed again and so on, as the product of strategic interaction between active opponents.

There is a lot to like here. Lindsay's argument contributes to arguably the most important trend in the last two decades of military effectiveness research: growing attention to the role of non-material variables. Security studies had once treated military capability through simple materialist bean counts of troops, or expenditures, or population, or GDP – and official Defense Department models are still, to this day, largely materialist in their treatment of military outcomes. A generation of ongoing research has challenged this materialist view, demonstrating the importance of nonmaterial variables such as force employment, culture, regime type, human capital, political ideology, social structure, ethnicity, institutional design, civil-military relations, global norms, international systemic competition, economic development, alliance structure, logistical choices, and more.[1] Yet much remains to be done. And among the most important unexplored possibilities for important

[1] See, for example, Risa Brooks and Elizabeth Stanley, eds., *Creating Military Power: The Sources of Military Effectiveness* (Stanford: Stanford University Press, 2007); Dan Reiter, ed., *The Sword's Other Edge: Trade-offs in the Pursuit of Military Effectiveness* (New York: Cambridge University Press, 2017); Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004); Dan Reiter and Allan C. Stam III, *Democracies at War* (Princeton: Princeton University Press, 2002); Caitlin Talmadge, *The Dictator's Army: Battlefield Effectiveness in Authoritarian Regimes* (Ithaca: Cornell

non-material contributors is precisely the issue Lindsay takes on: information practice, and the ways in which real militaries use the information technologies that are such an increasing focus of the defense policy debate in the United States and elsewhere. This has begun to attract attention, particularly in the naval warfare literature.[2] But the nonmaterial dimension of information in war remains a major gap in the growing military effectiveness literature, and Lindsay's book takes an important step toward filling it.

Lindsay's argument, moreover, is persuasive and important. And his case studies are impressive in their depth and ability to capture the subtle nuances of the way real organizations use information technology. In fact, his Iraq case study approaches the status of an anthropological ethnography of information practice, benefitting from his status as a participant observer during his tour of duty as an officer with an intelligence detachment operating in support of a special operations task force (SOTF) in Anbar Province. Case studies in political science rarely evoke a sense of place, but this one does. I've spent a fair amount of time in a variety of headquarters units and assessment cells in both Iraq and Afghanistan, and not only did everything Lindsay say about the SOTF in Anbar ring true, but his theoretical analysis explained, far better than any other account I've read, not just what I saw in other headquarters, but why, and why these organizations produced the results they did in their efforts to understand their environments. I learned a lot from all his case studies, but especially so for the chapter on Iraq.

University Press, 2015); Jasen Castillo, *Endurance and War: The National Sources of Military Cohesion* (Stanford: Stanford University Press, 2014); Michael Desch, *Power and Military Effectiveness: The Fallacy of Democratic Triumphalism* (Baltimore: Johns Hopkins University Press, 2008); Jonathan Caverley, *Democratic Militarism: Voting, Wealth, and War* (New York: Cambridge University Press, 2014); Kenneth M. Pollack, *Arabs at War: Military Effectiveness* (Lincoln: University of Nebraska Press, 2002); Stephen Peter Rosen, *Societies and Military Power: India and Its Armies* (Ithaca: Cornell University Press, 1996); Risa A. Brooks, *Political-Military Relations and the Stability of Arab Regimes,* Adelphi Paper 324 (Oxford: Oxford University Press, 1998); Elizabeth Kier, *Imagining War* (Princeton: Princeton University Press, 1997); Allan Stam, *Win, Lose or Draw* (Ann Arbor, MI: University of Michigan Press, 1996); John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983); Ryan Baker, *Logistics and Military Power: Tooth, Tail, and Territory in Conventional Military Conflict* (PhD dissertation, George Washington University, 2020); Allan Millett and Williamson Murray, eds., *Military Effectiveness*, 3 vols. (Cambridge: Cambridge University Press, 1998/2010); Anthony Pascal, *Are Third World Armies Third Rate? Human Capital and Organizational Impediments to Military Effectiveness* (Santa Monica, Calif.: RAND, January 1980); Stephen Biddle and Stephen Long, "Democracy and Military Effectiveness: A Deeper Look," *Journal of Conflict Resolution* 48:4 (August 2004): 525-46; Alexander B. Downes, "How Smart and Tough Are Democracies? Reassessing Theories of Democratic Victory in War," *International Security* 33:4 (Spring 2009): 9-51; Michael Beckley, "Economic Development and Military Effectiveness," *Journal of Strategic Studies* 33:1 (February 2010): 3-79; Theo Farrell, "World Culture and Military Power," *Security Studies* 14:3 (2005): 448-488; Jeffrey A. Friedman, "Manpower and Counterinsurgency: Empirical Foundations for Theory and Doctrine," *Security Studies* 20:4 (2011): 556-591; Elizabeth Kier, "Homosexuals in the U.S. Military: Open Integration and Combat Effectiveness," *International Security* 23:2 (Fall 1998): 5-39; Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75:2 (1996): 37-54; Barry R. Posen, "Nationalism, the Mass Army, and Military Power," *International Security* 18:2 (Autumn 1993): 80-124; Bryan C. Price, "Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism," *International Security* 36:4 (Spring 2012): 9-46; Patrick B. Johnson, "Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns," *International Security* 36:4 (Spring 2012): 47-79; Jenna Jordan, "When Heads Roll: Assessing the Effectiveness of Leadership Decapitation," *Security Studies* 18:4 (2009): 719-755; Barry Posen, "Measuring the European Conventional Balance: Coping with Complexity in Threat Assessment," *International Security* 9:3 (Winter 1984/85): 47-88; John Mearsheimer, "Assessing the Conventional Balance: The 3:1 Rule and its Critics," *International Security* 13:4 (Spring 1989): 54-89; Joshua Epstein, "The 3:1 Rule, the Adaptive-Dynamic Model, and the Future of Security Studies," *International Security* 13:4 (Spring 1989): 90-127.

[2] See, for example, Norman Friedman, *Network Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars* (Annapolis: Naval Institute Press, 2009); Trent Hone, *Learning War: The Evolution of Fighting Doctrine in the U.S. Navy, 1898-1945* (Annapolis: Naval Institute Press, 2018), esp. 208-249; Michael Palmer, *Command at Sea: Naval Command and Control since the Sixteenth Century* (Cambridge: Harvard University Press, 2007).

Of course, no book is perfect, and there are always things that could have been done better if authors had unlimited time and space. Here, the case studies sometimes suffer the weaknesses of their strengths: the very detail of their ethnographic description can make their theoretical function harder to follow. The connection between the deductive theory and the empirical discussion is not always as clear as it could be; control of extraneous variance is imperfect (note Lindsay's own list on 247); and it is not entirely clear whether the cases are meant to test the theory (243, 246) or merely as illustrations of its features or of the process of its discovery (71, 243-48). In principle the cases could be tests, illustrations, and inspirations at the same time, as Lindsay notes in his discussion of abduction (244-45). But the requirements for a dispositive test are much more demanding than those for illustration or discovery, and it is unclear whether those requirements are always met here, or how much power this test provides given the features of the cases chosen – the case selection discussion (243-48) is stronger on Lindsay's own voyage of discovery than it is on the fit between the cases ultimately chosen and the usual criteria for selection in testing. That said, Lindsay's candor in describing the process of discovery is refreshing – as he points out, most of us airbrush out the process that got us to our findings in the interest of economy in presenting them. Lindsay's discussion here may help reassure many Ph.D. candidates as they wrestle with the reality of research as opposed to the archetype typically presented in methods courses.

It also would have been helpful if Lindsay had clarified the relationship between the book's stated dependent variable (information practice) and its unstated dependent variable of victory in battle. The latter is why we care about the former, and Lindsay clearly recognizes this. As a result, the text sometimes veers into an implicit discussion of victory and defeat (for example, 72) but without any explicit treatment of what is surely a complex relationship between battle outcomes and variations in information practice or its causes.

This elides perhaps the most important question many readers will have for the book: how important is information practice, relative to other things, for success in battles or wars? The military effectiveness literature is centrally about the overarching question of what causes victory. I find the book interesting largely because it promises insight into this overarching question in an era in which many voices claim that new information technology will be decisive in war. Lindsay's analysis is deeply skeptical of this claim, and I tend to agree with him on this. But that leaves unanswered many other big questions for the subject. Does sound information practice matter more than superior numbers or firepower? Does it matter more than sound maneuver tactics or morale or logistical support or combat arms training? How much of a difference does information practice really make?

That said, all good books inspire questions beyond those they ask and answer, and no book answers every question it raises. We all study aspects of the world, not its entirety. And for an area such as information practice, which to date has attracted limited scholarly attention, it is a reasonable choice for Lindsay to carve off a piece of this domain – the relationship between information practice and its causes – and study that. But I hope that he, or others that he may inspire, will take the analysis further in future work and tell us how much this matters, and how it relates to combat outcomes as a whole.

When Lindsay or others do this, there are a variety of other possible implications that will flow from this broader answer. Major decisions in force design, unit organization, and resource allocation turn on the relative importance of information practice as opposed to everything else a military does.

The book's discussion of "the informational turn in war" (28-31) is especially interesting on this score. The text here argues that information is increasingly important for outcomes, and hints that perhaps it is already more important than many other contributors, though it does not try to establish this via dispositive evidence. But it also hints at a powerful coming culture shock for many world militaries. In this discussion, Lindsay frames war, increasingly, as office work: "[T]he battle rhythms of military organizations have converged with the corporate routines of administrative offices" (30). War, increasingly, is practiced from swivel chairs at desks in reasonably safe locales by teams that may include as many civilians as officers, all staring at computer monitors and using Microsoft Office products to email one another briefing slides. The heroic model of warriors closing with the enemy in mortal exertion on the battlefield has been suffering for decades, if not centuries, but Lindsay's analysis points to an earlier demise for this ideal than many military organizations are ready for.

If Lindsay is right, one can get a sense for the coming military *kulturkampf* from the 1980s debate over "military reform." The reformers saw the post-Vietnam U.S. military as dominated by bloodless managers and corporatist military bureaucrats who valued 'servicing targets'and had lost the warrior spirit. The reformers caught the imagination of a generation of officers who were frustrated by what they saw as an overemphasis on orderly administration and who longed for inspiration in what the Wehrmacht had called "the free creative art of war."[3] The U.S. Army's maneuverist AirLand Battle doctrine of 1982 was a direct outgrowth of this, and the speed with which the military embraced the reformist critique speaks to a deep vein in Western military culture and its resistance to the image of war as mere office work.[4] Epithets such as the age-old "REMF" (rear echelon mother-f*****) or the more recent "fobbit" (referring to those who serve on large forward operating bases, or FOBs) reflect the same set of norms. Anton Myrer's novel *Once an Eagle* is often cited as an unusually perceptive window on U.S. Army culture in particular; Myrer's protagonist is a muddy-boots soldier who rises to high rank through heroic feats of personal courage in battle, and whose chief antagonist is an over-educated staff officer who schemes from safety in the rear while torturing small animals.[5]

This reverence for muddy boots soldiering at the front has always undervalued the importance of good staff work in the rear: General George Patton's maneuverist brilliance in counterattacking into the base of the German salient in the Battle of the Bulge in 1944 was enabled by the careful analysis of a very talented team of staff officers who quickly figured out the myriad of administrative details required to turn an army ninety degrees while remaining in contact without causing massive fratricide or logistical chaos; the information practice in Patton's headquarters made his maneuvers possible. But for many officers today, it is Patton's ostensible creative genius at the art of war – not his staff's proficiency in military office work – that gets the credit and comprises the role model to be emulated. If Lindsay is right – and if the importance of information practice relative to other things is as great as Lindsay hints in *Information Technology and Military Power* – then Western military culture is headed for a major reckoning. And if so, then military success in the future could well turn on forces' ability to manage this cultural transition at least as much as it will depend on the sophistication of their weapons or equipment, or their free creativity in the art of war.

[3] *Heeresdienstvorschrift 300, Truppenfuhrung ["Troop Leadership"]* (Berlin: Verlag Offene Worte, pt. 1, 1933), 1.

[4] On the military reform movement, see, for example,, Asa Clark et al., eds., *The Defense Reform Debate* (Baltimore: Johns Hopkins University Press, 1984); James Fallows, *National Defense* (New York: Vintage, 1982); William S. Lind, *Maneuver Warfare Handbook* (Boulder: Westview, 1985).

[5] Anton Myrer, *Once an Eagle* (New York: Harper Perennial, 2013 [1968]).

Review by Audrey Kurth Cronin, American University

Jon Lindsay's captivating book concerns the organizational and human challenges of the collection, analysis, sharing, and employment of data and information for military strike missions in the digital age. At the intersection of information technology and military power, Lindsay's book focuses on what is lost in translation between evidence gathering and analysis, and then distorted or absent in dissemination and implementation. His study stresses the targeting of individuals or military objectives, drawn from the author's experience as a U.S. Naval officer specializing in intelligence and information technology, especially during deployments in Iraq and Kosovo (2007-2008 and 1999).

Knowing why some military organizations adapt to changing circumstances and others fail to do so is essential to understanding outcomes in war. Throughout the book, a key theme is the role of human innovation during conflicts, or what (in programming jargon) the author calls "runtime design." (63,133). This concept has a lengthy history in warfare[1] and is likewise crucial to computer-assisted operations in the digital era. With fascinating insight into recent U.S. military operations, Lindsay's book contributes fresh evidence for researchers at the intersection of organizational theory, information practice, and the changing character of war.

Like most American political scientists these days, Lindsay follows the introduction with a heavy dose of theory. The first chapter is an examination of the "Technology Theory of Victory," by which he means the view that "computational networks will determine success or failure," and explains alternatives to this theory (13). He reviews organizational behavior and information practice across disciplines, emerging in chapter 2 with four patterns common to how militaries employ new technology, namely 1) managed practice; 2) insulated practice; 3) problematic practice; and 4) adaptive practice (32).

These categories are crucial to victory, Lindsay argues, because how military organizations collect, handle, and disseminate information determines their effectiveness. Managed practice and adaptive practice improved military performance; insulated practice and problematic practice undermine it. "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," he asserts (50). Control of information is crucial to victory.

The heart of the book, chapters 3-6, is anchored in four case studies, including the use of radar during the Battle of Britain (1940), user innovation of FalconView Aviation Mission Planning Software (the 1980s-2000s), direct action by U.S. special operations in the occupation of Iraq (2003-2008), and U.S. post-9/11 targeting of armed drones (2001-2018). The middle chapters introduce material drawn from the author's service as a naval officer. I found them rewarding.

The story of FalconView in Chapter 4 describes military innovation and diffusion of affordable, accessible software at the end of the twentieth century. Like thousands of civilian hobbyists, air force pilots participated in the personal computer (PC) boom of the 1980s by buying cheap personal desktops, then writing, experimenting with, and sharing flight-planning software. A decade in, U.S. Air National Guard members joined programmers at Georgia Institute of Technology to formalize these spontaneous efforts, writing a software application for the F-16 Fighting Falcon (thus FalconView). FalconView sprouted an array of intelligence and planning applications, especially when combined with Microsoft Office

[1] Stephen Rosen examines wartime innovation in the first and second world wars in *Innovation and the Modern Military: Winning the Next War* (Ithaca: Cornell University Press, 1991). Counterinsurgency literature often focuses on human innovation during conflict, though not directly on the role of technology. See for example, David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger, 2006); John Nagl, *Learning to Eat Soup with a Knife* (Chicago: University of Chicago Press, 2002). Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency* (New York: Praeger, 2006); and more recently, David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2011); and Carter Malkasian, *War Comes to Garmser: Thirty Years of Conflict on the Afghan Frontier* (Oxford: Oxford University Press, 2013).

extensions. Amateur users, especially reservists who were transitioning from civilian life, were skilled at adapting commercial devices and software for day-to-day military uses.

What emerged was a suite of geospatial tools using GPS and tactical radio feeds to produce maps and charts, similar to Google Maps. As the software was unclassified, users could install it on their personal laptops, share it with allies and colleagues, and further tinker with it—yielding still more maverick applications. This was fast, effective, bottom-up innovation, as creative as in any start-up, thriving within the military when Silicon Valley had begun to outpace traditional military acquisition. FalconView delightfully demonstrates the clash between what Lindsay calls organic and institutionalized approaches—essentially bottom-up and top-down innovation. It is easy to conclude that military user innovation is the way to go.

Yet the stakes in military technology differ from those in Silicon Valley start-ups. Secuity risk is the downside of open innovation, made evident when Chinese hackers stole the FalconView software in 2005. A heightened concern with adversary breaches spurred Pentagon bureaucrats into action, shifting momentum toward top-down acquisition, snuffing out personal initiative even as they failed to improve cybersecurity, according to Lindsay. It is a classic tale of first mover disadvantage. While not directly addressing how to handle complex tradeoffs, Lindsay strikingly lays them out for the reader to ponder. The answer is not simply to let organic innovation rule the day, he avers, since individual software solutions may be fragile, nontransferable, unscalable, or insecure.

An equally outstanding chapter follows. It examines Naval Special Warfare (NSW) operations in Anbar province, Iraq, where the author deployed in 2007-2008 with a Navy SEAL Team as part of a Special Operations Task Force (SOTF). Lindsay describes a pervasive bias for direct action emerging from the Navy SEALs' aggressive culture, incentives, and selection process. Operators were hungry for targets, and technical analysts were eager to produce them, so neither probed the shaky intelligence upon which they were based.

Short tours only made matters worse. Analysts transitioned in and out every six months, few spoke Arabic, most relied on translation machines or Iraqi interpreters with potential personal agendas. Reports were littered with mistakes or omissions, such as misspelled names or unknown tribal lineage. Impressive network charts resembling giant “hairballs” (162) appeared on the walls, suggesting technological prowess yet built on dubious data.

Digital communication intended to improve effectiveness thus ended up perpetuating a cycle of targeting, Lindsay argues. Information management in SOTF was chaotic. Computer filing systems were so disorderly that paper copies became essential. Headquarters’ television links drew real-time attention to heroic SEAL missions but not to longer-term assessments, such as whether the person captured yielded good intelligence or was even the right guy. Lindsay contrasts the technology-intermediated practice with the actions of nearby U.S. Marines, who took a low-tech policing approach, physically moving among the population and collecting information that could be checked and corrected as they went along. With SOTF’s secluded, computer-focused approach, he writes, “Questions about targeting performance were difficult to answer, and the asking was not encouraged” (178).

In Anbar, digital means detached tactics from strategy. The official process for special operations was to “find, fix, finish, exploit, analyze” (or F3EA) (154)—but the author argues the last two steps were rarely taken. There was no effective feedback loop to determine whether capturing or killing targets made Anbar politically more or less stable, a mistake I believe played a role in the rise of the Islamic State a few years later.

These two hard-hitting chapters draw upon Lindsay's personal experience, which shows in the depth of his analysis and the rich detail with which he fleshes out each point. The Battle of Britain (chapter 3) is well handled and interesting but strikes me as the odd one in this mix. In 1940, the British were the ones targeted by the Germans, not the other way around. The UK fought for its life, suffering withering attacks on its soil, especially in its capital city. This was not an effort to gain information ‘control’ but to protect the population and survive, using proprietary defensive technology—radar—along with a fully mobilized, networked society enabling it to work. The will of the British people was at stake here, and the outcome depended as much on psychology and politics as it did on technology.

On the other hand, Chapter 6, on the U.S. drone campaign, is very much a targeting mission that follows well upon the heels of the special operations chapter. Lindsay presents it as a successful example of managed practice, where drone operators feel the flow of battle and gain close familiarity with targets. He details the multi-layered process of target approval, extending to the president during the Obama administration, and he also explores the ethical and legal questions of targeting U.S. citizens. Lindsay distinguishes between individually targeted drone strikes (personality strikes) and less discriminate attacks on groups of militants who meet a specific profile (signature strikes). He concludes, "Yet more complexity and tactical precision do not translate into reliable strategic advantages and legitimate outcomes" (211), an observation with which I heartily agree.

That brings me to two minor quibbles in this otherwise excellent book. First, the term Revolution in Military Affairs (or RMA) is used loosely throughout. Lindsay writes that "this book turns the RMA inside out by examining how people conduct war in an information-intensive environment" (6). I am not sure what that means. The RMA was a set of theories that were popular in the United States military (especially the Navy and Air Force) in the late 90s, asserting that a system of US-dominated information age technologies would "lift the fog of war" and yield victory through "dominant battlespace knowledge, near-perfect mission assignment, and immediate/complete battlespace assessment."[2]

Does anyone still believe that fantastical notion? Local political contexts in post-9/11 Iraq and Afghanistan were more complex than any sensor-based digital technology could render 'transparent.' Even high-technology, capital-intensive Services such as the Air Force and the Navy have long moved beyond claims of one-sided, technology-driven dominance. The author frequently asserts this exact point—that political context belies overreliance on digital technology. I would have preferred that he omitted RMA jargon altogether.

My second reservation regards periodical references to Carl von Clausewitz's theories, which could not be more at odds with the book's argument about control. He states, "War features extreme competition between opposed organizations of cooperators. People in a military organization try to cooperate to avoid control failures, while their external competitors seek to cause them" (68). But in *On War,* Clausewitz argues that war is a contest of wills, violence is at the heart of it, confusion is inevitable, and control is impossible; "As a total phenomenon its dominant tendencies always make war a paradoxical trinity—composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone."[3] Lindsay analyzes war as a competition between military organizations while Clausewitz argues it is a competition between *societies*.

These observations aside, Jon Lindsay's *Information Technology & Military Power* offers a shrewd analysis of and invaluable evidence about how information is used in militaries today. This excellent volume should be broadly read, as its arguments reach beyond the study of military innovation, cyber warfare, or information technology and will have staying power. It offers insight into why the so-called 'war on terror' became so heavily dependent on impressive military tools and lost its bearings. American fascination with technology has led to a tactical focus that belies clear thinking about longer term goals and outcomes. The author demonstrates that separating information-gathering and manipulation from the political purpose of warfare inevitably undermines strategic success. The answer is not to abandon information technology but

[2] Bill Owens with Ed Offley, *Lifting the Fog of War* (Baltimore: Johns Hopkins University Press, 2000), 100. I have omitted the italics in the original.

[3] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret, Book 1, Chapter 1 (Princeton: Princeton University Press, 1976), 89. Chapter One, the only one that Clausewitz himself considered finished, ends in this culmination of his argument.

instead to harness it in the service of long-term national goals--an endeavor that reaches beyond recent wars and extends deep into the future of American democracy.

Review by Myriam Dunn Cavelty, Center for Security Studies, ETH Zürich

Jon Lindsay's *Information Technology and Military Power* is many great things. It is an eloquent book about the Revolution in Military Affairs with a twist, because it looks at people using technologies,a not at technologies determining the actions of people. It is an empirically rich study of military success and failure and an at times charmingly auto-ethnographic account of experiencing information friction while serving in the U.S. military. It is a theoretically innovative take on the challenges of digital transformation in the public sector. Not least, it is a passionate plea against letting technological determinism as manifest in the 'technology theory of victory' guide our thinking about military power.

The 'technology theory of victory,' which is challenged in chapter 1 of the book, is the stubbornly pervasive and cyclically arising belief that "computational networks will determine success or failure" (13).[1] Undoubtedly, the U.S .is the most technologically advanced military power in the world. Why then has it struggled so much against much weaker adversaries despite its information technological advantages? Lindsay's answer to this puzzle is as simple as it is complicated: 'It's the context, stupid!' Seeing how "the political power of a state or organization is a product […] of the representational system that produces actionable knowledge about the world" (37), military power arises as a function of how well the organization manages to match its technologies to the environment they operate in.

Skilfully weaving together theoretical ideas from a variety of literatures and disciplines in chapter 2, Lindsay sets out to enhance our understanding of the relationship between information technology and military power via a "theory of information practice." He defines it as "sociotechnical pattern of organizational behavior that coordinates the relationships between internal representations and the external world" (33). The framework the book presents to us consists of four distinct patterns: managed practice, insulated practice, adaptive practice and problematic practices. Managed and adaptive practices enhance military performance, insulated and problematic practices undermine it (56). Each type of practice is defined by either a match or a mismatch between the warfighting problem and the organizational system. In managed practice, the problem is well structured and understood and the organizational system is well adapted to it (57). Practice is insulated when the organizational culture is too rigid for a dynamic or ambiguous environment (58). This can be fixed by creative, unorthodox solutions, which are called adaptive practice (62). Problematic practice, finally, differs from insulated practice on the point that the people in the organization are aware of the deficiencies of their practices (65).

Four detailed case studies (chapters 3 to 6) illustrate the four patterns. Unfortunately, the guiding principle of the case selection remains unclear and even appears somewhat eclectic, not least because the chapter that builds on a previously published paper reads like an insert that is mostly detached from the framework.[2] One is left wondering what scientific purpose the in-depth illustrations serve since they are selected on the dependent variable, not to challenge but merely to illustrate and reinforce the assumptions made in the theoretical framework. Since each case looks mainly at one pattern of information practice, Lindsay also cannot substantiate his intriguing claim that "organizations tend to cycle through all four patterns as external and internal actors engage in disruptive exploitation and stabilizing reform" (56) though there is some information practice mix in his chapter 5.

If one reads beyond the last word of the conclusion, one realizes that some of the questions about the mode of social inquiry (abduction), the innovative method that Lindsay used predominantly (ethnography) and, to some degree, the reasoning

[1] There were a lot of publications arguing in favour of this simplistic link, especially in the 1990s. A few relevant examples include: Stuart E. Johnson and Martin C. Libicki, *Introduction to Dominant Battle-Space Knowledge: The Winning Edge* (National Defense University, 1995); John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND Corporation: 1997); Joseph S. Nye Jr. and William A. Owens, 'America's Information Edge', *Foreign Affairs* (March/April 1996): 20-36.

[2] The paper is: Jon R. Lindsay, "'War upon the Map': User Innovation in American Military Software," *Technology and Culture* 51:3 (2010): 619-651.

behind the case selection are answered in the appendix ("methodology," 243-248). It is unfortunate that this chapter is mentioned solely in footnote 5 of the introduction. It definitely deserved a more central position in the book because every point made on those few pages is crucial for understanding Lindsay's approach and overall aim and should guide our appreciation of the book's undoubtable scientific value as well as the practical implications for policymakers and shapers it suggests.

Overall, Lindsay's book fits an important trend in the literature on military innovation and technology and at the same time adds important facets to it that were previously neglected or not as clearly elaborated.[3] The biggest remit of *Information Technology and Military Power* lies in its tireless effort to highlight organizational struggles to coordinate knowledge and control and to illustrate how mismatches between problems and technological solutions create information friction. Chapter 7 deserves particular praise for linking theoretical propositions to practical implications in a systematic and approachable way. What this book makes clear it that technological hubris as encapsulated in the 'technology theory of victory' is not just an intellectual problem – it is very much a practical problem, on a tactical, operational and strategic level. That the very technologies an organization uses to optimize its performance become a potential source of failure is the most important lesson to take home.

However, the situation seems to be even worse. As Lindsay notes, speaking from experience, "military personnel have become increasingly preoccupied with the frictions and breakdown produced by the complexity of the information systems that enable them to know and influence the battlefield" (214). It is perhaps telling that the two success cases in the book are a historical one, looking at the Royal Air Force (RAF) Fighter Command during the Second World War, and the history of a platform that trumped over other solutions, FalconView, rather than an actual military operation. Information friction, so it seems, is simply inevitable in an age of complex systems. Thus, the question is not how to prevent it – but how to "turn friction into a source of traction that enables people to improve their systems" (217).

The book outlines two "solutions" for this conundrum: find and train socio-technical geniuses and learn how to be adaptive. While the "hackers are geniuses" myth is probably another recipe for disaster rather than a solution given how variable this stereotypical take on technologically interested individuals and groups is,[4] adaptive management practices fit the book's focus on the organizational need to react the right way.[5] I want to highlight just a few of Lindsay's points here. For him, solutions, just like in the information practice framework, can be institutionalized (or top-down) or they can emerge more organically (bottom-up). What Lindsay advocates, for example, is an institutional support system for tech-savvy personnel so that they can more easily adapt the organizational system if it underperforms. He also envisages the deployment of operational hackers "as far forward as possible" (224) and more openness to use commercial technology whenever feasible.

However, the limits of Lindsay's deliberately simple theoretical framework become obvious at this point. He chooses to explain the success or failure of military combat operations exclusively via the match or mismatch between the

[3] For simplicity, we can call the trend a 'Science and Technology Studies (STS) inspired take on the difficulty to make technologies work.' Prominent examples are: Andrea Gilli and Mauro Gilli, **"**Why China Has Not Caught up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43:3 (2019): 141-189; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment", *International Security* 41:3 (2016/2017): 72–109; Daniel R. McCarthy (ed.). *Technology and World Politics: And Introduction* (Routledge, 2018). Also, for an early take on looking at knowledge processes in laboratory settings; Donald Mackenzie and Graham Spinardi, "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons." *American Journal of Sociology* 101:1 (1995): 44-99.

[4] Leonie Maria Tanczer, "50 Shades of Hacking: How IT and Cybersecurity Industry Actors Perceive Good, Bad, and Former Hackers", *Contemporary Security Policy* 41:1 (2020): 108-128.

[5] For an interesting framework that uses complexity thinking to link decision-making styles to system states, see David J. Snowden and Mary E. Boone, "A Leader's Framework for Decision Making," *Harvard Business Review*, November 2007: 1-8. Also explained here: https://www.youtube.com/watch?v=N7oz366X0-8 .

organizational solution and the external environment. In turn, this leads to the unidirectional reasoning that in case of a mismatch, the organization has to adapt its practices reactively in order to better match the environment. This assumes not only that we can separate the internal subsystem (the organization) from the external (the environment) in theory and in practice, but also that we can easily distinguish between reality (situated out there in the environment) and representations of it (in here in the organization's systems). Such a distinction is problematic because it overlooks another, potentially more consequential source of information friction.

It is cognitively satisfying to believe in the existence of an objective 'truth' outside and beyond of human observation. It allows us to strive towards reducing uncertainties about threats with 'better' data collection practices that lead to the 'better' representation of threats. Granted, in the example of fighter planes in a geographically limited theater of war that we find depicted in the book, there is relatively little uncertainty about the enemy, their intent, and the tools they want to use to project force. However, are these controlled environments the norm or the exception in today's and future conflicts? No, we are mainly challenged by conflictual settings that bring into question the traditional, cognitively clear categories and assumptions about amity-enmity, internal-external spheres of influence, war-peace etc. and the very tools we use to achieve our political goals. Therefore, if "information is a complex pragmatic relationship between representations and reality" (48) then we need to take into account that information practices can be transformative of the environment as well – or maybe even construct it in the first place.

Critical intelligence studies are an interesting place to turn to for more insights about the interplay between information practices, preconceived assumptions, and particular effects.[6] One of the most studied phenomena in the intelligence literature writ large are 'intelligence failures,' which bear a great resemblance to Lindsay's concept of "information friction." To avoid 'failures,' the literature assumes that we need to identify the sources of friction in the system of knowledge production and then optimize it accordingly to reduce the probability of such failures in the future. Critical intelligence scholars hold against this that we should study the interplay between knowledge creation practices and the objects ('threats') they purportedly study. There is no such thing as 'raw data,' a representation of reality that is enriched in the intelligence process to reduce uncertainty about the world: Data is already always taking a particular shape before collection even starts due to the decisions taken about what to collect.[7] Maybe there is no red or blue pill like in the film *The Matrix* but only a purple pill. In an era of post-truth, the very practice of producing actionable knowledge about the world co-constructs the world. Politically impactful information friction arises from the attempts to establish the truthfulness of one representation over another, potentially undermining the very foundation of an organization.

In sum, and my points of critique notwithstanding, *Information Technology and Military Power* is a valuable and much needed invitation to delve deeper into the complex and intriguing relationship between organizations, information technologies, and the practices that arise from their use. One of its key merits is the convincing destabilization of the 'vampire fallacy' that grants technologies transformative powers without considering the context of their use.

[6] For an overview see Bean Hamilton, "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had," *Intelligence and National Security* 33:4 (2018): 527-540.

[7] Minna Räsänen and James M. Nyce, "The raw is cooked: Data in intelligence practice*," Science, Technology, & Human Values* 38:5 (2013): 664.

Review by Paul N. Edwards, Stanford University

Long ago, when I was writing *The Closed World* (1996),[1] two masterpieces of military analysis stood out to me above all others: Paul Bracken's *The Command and Control of Nuclear Forces* (1983) and Martin van Creveld's *Command in War* (1985). Both readily bear re-reading today. I can still recite from memory several key sentences. Bracken: "The likelihood of nuclear Munichs has been exaggerated, but the possibility of nuclear Sarajevos has been understated."[2] He meant that while both American and Soviet strategists obsessed over preventing nuclear blackmail by a superior force, they attended much too little to how, in the midst of some fraught crisis, misinterpretations and errors could lead to rapid escalation, all the way to Defcon 1. Around that same time, computer scientist Alan Borning and others began to document in terrifying detail the many moments when American warning systems came within a hair of launching a nuclear first strike due to computer errors and human-computer interactions.[3]

Van Creveld, on the "information pathologies" of 1960s military practice: "The trend toward statistics was probably enhanced by the very size of the information flow needed to run the war in Vietnam, leading to a situation in which messages could not be read but had to be counted instead. …Statistics, even when accurate, can never substitute for in-depth knowledge of an environment, a knowledge that the Americans in Vietnam were almost entirely without."[4] Dangerous field situations, combined with commanders' and Defense Department leaders' requirements for more "information," generated dysfunctional incentives which encouraged massive over-reporting of enemy casualties and infrastructure damage by aerial bombardment. Meanwhile, the prestige of then-new computer analysis lent a veneer of validity and power to "information" that was in fact little more than distorted, self-serving speculation converted to numerical form.

I read and re-read these fascinating texts not only for the brilliance of their analysis, but also because these men were extraordinary writers, gifted with insight, clarity, and style that cut like samurai swords through the jargon-laden, coma-inducing strategy documents of the American military leadership and its industrial clients. For those same reasons, Jon Lindsay's book now joins these earlier masterworks on my (mostly virtual) bookshelf. It may even eclipse them.

Lindsay's background provides him with exceptional authority on his subject. He holds a BS degree in Symbolic Systems and an MS in Computer Science, both from Stanford University. Unlike most academic political scientists, he served seven years as an intelligence officer in the US Navy, followed by another ten years in the US Naval Reserve under the intimidating title of "Information Dominance Warfare Officer." During his reserve service, he acquired a Ph.D. in political science from MIT. Lindsay spent four years at UC San Diego's Institute for Global Conflict and Cooperation, founded by former Los Alamos physicist and national security analyst Herb York.

On top of that, Lindsay has read *everything.* He canvasses entire literatures on military strategy and command, organization theory, computer-supported cooperative work, human-computer interaction, and science & technology studies (STS). He cites sociologist-philosopher Bruno Latour as fluently as 19th century Prussian general Carl von Clausewitz, economist

[1] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge: MIT Press, 1996).

[2] Paul Bracken, *The Command and Control of Nuclear Forces* (Bethesda: World Future Society, 1983), 2.

[3] Alan Borning, "Computer System Reliability and Nuclear War." *Communications of the ACM* 30:2 (1987): 112-31; Michael D. Wallace, Brian L. Crissey, and Linn I. Sennott. "Accidental Nuclear War: A Risk Assessment." *Journal of Peace Research* 23:1 (1986): 9-27; David L. Parnas, "Software Aspects of Strategic Defense Systems," *Communications of the ACM* 28:12 (1985): 1326-1335.

[4] Martin Van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 252-253.

Friedrich Hayek as easily as sociologist Charles Perrow, and psychologist William James as readily as human-computer interaction specialist Ed Hutchins. In short, he knows what he's talking about.

Much of what we call "information technology" can be understood as automating routines and procedures previously carried out by human beings. Initially this automation appeared as simple efficiency gains, but the further it proceeded, the more it generated qualitative differences in how organizations operate, structure their communications practices, and understand their missions.[5] Over the past sixty or seventy years, this transformation has affected virtually all large organizations, from weather services to government agencies and hospitals to the computer industry itself, often in similar ways. Since the 1990s, one miracle of the Internet has been the automation of routines that exist *between* organizations, for example in closely coordinating global supply chains consisting of hundreds of firms.

Yet this characterization in terms of 'automation,' common (and accurate) as it may be, misses a salient aspect of how that automation actually works. Old routines are automated, but that process virtually always generates *new* routines for human organizations — as well as new, often time-critical issues that must be resolved by human workers through improvisation, user innovation, or retreat to older, better understood routines. You yourself are a tiny microcosm of this much larger issue. Unless you have inhabited a computerless cave for the last six months, you have with 99.9 percent certainty been forced to reboot your computer at least once, update software, adopt new software, fix some mystifying technical failures, improvise ways to make incompatible pieces of software work together, and learn to manage Zoom meetings as your own organization responds to the coronavirus pandemic. Intellectual giants such as Herbert Simon (*The Sciences of the Artificial,* 1968), Richard Nelson and Sidney Winter (*An Evolutionary Theory of Economic Change,* 1982), and Geoffrey Bowker and Susan Leigh Star (*Sorting Things Out: Classification and Its Consequences,* 1999) have all described these processes, noting the inevitability of breakdown and repair in information and communication systems of all sorts.[6]

Nowhere are these issues more salient, or more consequential, than in what Jon Lindsay calls the "information practice" (27ff) of military forces. The genius of Lindsay's analysis is to bring together a practice-oriented socio-technical systems analysis based deeply in Science and Technology Studies (STS) and organization theory with human-computer interaction theories such as "distributed cognition" (38ff) and carefully analyzed examples of actual information practice during military conflicts. He presents a series of simple — not simplistic — frameworks based on (a) what organizations can and cannot control about their own representations of reality, i.e. "information," (b) external situations that are relatively predictable and structured vs. those that are more fluid and unpredictable, and (c) the ways that technological change introduced to improve representations can lead to unanticipated distortions and misinterpretations, sometimes with deadly consequences such as casualties from "friendly fire" or the shooting down of civilian airliners mistaken for enemy aircraft.

A key focus of his framework is on the ever-increasing complexity of information handling in modern war. The ratio of logistics and information analysis personnel to frontline combatants has grown inexorably over the past century. In parallel, so has the number of interacting sensors, effectors, and supporting information systems. Together, these phenomena have increased "information friction" (2ff) in Lindsay's terms. Remote-controlled, precision-guided weaponry and high-tech surveillance systems have greatly reduced frontline troop casualties, simply by reducing the number of personnel who are directly involved in combat. Yet the information friction involved in ensuring that surveillance data reflect the realities they are supposed to represent has often led to failures of what Lindsay calls "referential integrity" (46ff). The all-too-regular tragedy of civilian casualties inflicted by, for example, mistaking hospitals for Taliban strongholds testifies to ongoing breakdowns of referential integrity.

[5] Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Cambridge: Blackwell Publishers, 2000).

[6] Herbert A. Simon, *The Sciences of the Artificial* (Cambridge: MIT Press, 1996 [1968]); Richard R. Nelson and Sidney G. Winter. *An Evolutionary Theory of Economic Change* (Cambridge: Harvard University Press, 1982); Bowker, Geoffrey C., and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (Cambridge: MIT Press, 1999).

Lindsay's analysis is not merely a critique. His goal is to understand why information systems work well or poorly, where they produce gains or losses in military effectiveness, and how they can be improved. In this way his book resembles Diane Vaughan's masterwork *The Challenger Launch Decision*.[7] But where hers was a study of a single organization over a relatively brief period of time, Lindsay's framework is broad enough to encompass not only historical analysis — his first case study is the 1940 Battle of Britain — but also pragmatic ways to assess and improve present and future information practice.

In fact, as I suggested at the beginning of this review, his framework is broad enough to instruct nearly any organization that is confronted with changing information environments, i.e., basically every organization in the modern world. I would (and will) recommend this book, or at least its first two chapters, to schools of information, business, and engineering; computer science departments; STS programs; and of course to military historians and military schools. It could profitably be read by practitioners throughout the tech industry as well. In short, *Information Technology and Military Power* is a masterpiece.

[7] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: University of Chicago Press, 1996).

Response by Jon R. Lindsay, University of Toronto

Writing this book was a long and difficult process. I completely revised and rearranged it several times, and more than once considered abandoning it all together. Partly this was because I struggled to write one book for many different audiences—scholars and practitioners, political scientists and historians, positivists and interpretivists, realists and constructivists, and so on. Any effort to please all of them seemed doomed to leave everyone dissatisfied.

It is thus with considerable gratitude, and no little relief, that I read the contributions to this roundtable. I am both humbled and reassured to receive such thoughtful and encouraging comments from leading scholars in different disciplines. All of them have shaped my own thinking about technology or war in important ways. My ideas about technological mediation and information friction draw inspiration from Paul Edwards's award-winning histories of military and scientific computing.[25] To receive such high praise from a scholar of his stature is incredibly meaningful to me, and indeed somewhat vindicating given all the challenges experienced along the way. The title of my book is a direct reference to Stephen Biddle's seminal work on military power.[26] Biddle has a reputation as a tough reviewer, and he has spent a lot of time in the field with operational units, which naturally made me apprehensive about his reaction. I was thus gratified that he found the book "persuasive and important" and "a compelling account of an increasingly important issue." Ryan Grauer's book on military command (another titular homage to Biddle, and a significant contribution in its own right) encouraged me to stress the contingent fit between organizations and environments.[27] Myriam Dunn Cavelty's work has taught me a great deal about the follies of technological determinism in cyber discourse.[28] Audrey Kurth Cronin's scholarship on counterterrorism and drone warfare was also invaluable, especially for my chapter on drones.[29] Given publication schedules, I was sadly unable to cite Cronin's new book on the dark side of open technological innovation,[30] but I was thrilled to discover that she also explores the Janus-faced nature of user innovation. Finally, I am indebted to Rebecca Slayton for assembling such an

[25] Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge: MIT Press, 1996); Paul N. Edwards, *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming* (Cambridge: MIT Press, 2010).

[26] Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004).

[27] Ryan Grauer, *Commanding Military Power: Organizing for Victory and Defeat on the Battlefield* (New York: Cambridge University Press, 2016).

[28] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008); Myriam Dunn Cavelty and Andreas Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science," *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 5–32, https://doi.org/10.1080/13523260.2019.1678855.

[29] Audrey Kurth Cronin, "The Strategic Implications of Targeted Drone Strikes for US Global Counterterrorism," in *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, ed. David Cortright, Rachel Fairhurst, and Kristen Wall (Chicago: University of Chicago Press, 2015), 99–120.

[30] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (New York: Oxford University Press, 2020).

incredible roundtable. Her skillful integration of science and technology studies (STS) with security studies provides a model that all students of technology and security should aspire to emulate.[31]

The reviewers hail from different disciplines, each with different substantive interests and methodological commitments. This makes the generally positive tenor of their comments all the more gratifying. For perhaps the same reasons, they do not always agree about the books' strengths and weaknesses. For example, Cronin finds my chapter on automated mission planning "rewarding" and "outstanding" while Dunn Cavelty believes that it "reads like an insert mostly detached from the framework." Biddle and Cronin point out formulaic aspects of the book's organization: Biddle notes "the inescapable political science 2x2 table" while Cronin writes, "Like most American political scientists these days, Lindsay follows the introduction with a heavy dose of theory." Meanwhile, Edwards writes that he "would (and will) recommend this book, or at least its first two chapters, to" many different audiences. Edwards puts his finger on a central motivation of the book: "to bring together a practice-oriented socio-technical systems analysis based deeply in [STS] and organization theory with human-computer interaction theories." I was worried that I might have obscured this effort, if not sacrificed it altogether, in my attempt to translate these concepts into the idiom of international relations.

Dunn Cavelty highlights a central tension that I encountered in this translation. To once again sum up my "inescapable 2x2," my basic argument is that warfighting problems tend to be more or less constrained (structured, simplified, unchanging, etc.), while organizational solutions are more or less institutionalized (standardized, formalized, consensual, etc.). When organizations apply institutionalized solutions to constrained problems, military personnel are better able to understand and influence the battlefield; by contrast, unconstrained problems are better met with organic solutions that enable personnel to experiment and adjust. Mismatches between problems and solutions—institutionalized solutions to unconstrained problems or organic solutions to constrained problems—tend to create information friction (i.e., "the compromise of referential integrity resulting from collective action problems in the sociotechnical institutions of control" [48]), which degrades the quality of knowledge and control. Over time, as personnel and adversaries interact in peace and war, organizations tend to cycle through all four patterns. This dynamic tends to build up increasingly complex information systems, which produce increasingly frustrating information frictions.

Dunn Cavelty writes that "the limits of Lindsay's deliberately simple theoretical framework become obvious" once we begin "to question the traditional, cognitively clear categories and assumptions about amity-enmity, internal-external spheres of influence, war-peace, etc." She faults me for "unidirectional reasoning" and argues that "information practices can be transformative of the environment as well." Yet as it turns out, I am in complete agreement with her on these points. The very first paragraph of my theoretical chapter states, "The dependence or independence of these variables is ultimately an analytical convenience. Endogeneity…is inevitable because the members of an organization try to modify the same technologies that strategic competitors try to counter" (32). A long and turgid endnote in the same chapter begins with the caveat, "My distinction between internal and external factors does some violence to the richness of informational phenomena," before going on to cite some of the same pragmatist and phenomenologist philosophers who inform the general epistemological approach of "critical intelligence studies" (257, n. 37.) Dunn Cavelty commends this literature and warns that "There is no such thing as 'raw data'," even as one of my case studies observes that "raw intelligence was cooked from the get-go" (155), and we even cite the very same article to make these points![32]

I am thus very sympathetic to Dunn Cavelty's critique and regret that I could not better foreground my epistemological and ontological assumptions. Yet to do so might have risked alienating more positivist readers like Biddle. Biddle raises some important methodological questions about the "connection between the deductive theory and the empirical discussion," the

[31] See, for example, Rebecca Slayton, *Arguments That Count: Physics, Computing, and Missile Defense, 1949-2012* (Cambridge: MIT Press, 2013); and Rebecca Slayton and Brian Clarke, "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005," *Technology and Culture* 61:1 (April 4, 2020): 173–206, https://doi.org/10.1353/tech.2020.0036.

[32] Minna Räsänen and James M. Nyce, "The Raw Is Cooked: Data in Intelligence Practice," *Science, Technology, & Human Values* 38:5 (September 2013): 655–77.

"control of extraneous variance," and "whether the cases are meant to test the theory…or merely as illustrations." Biddle writes that it "would have been helpful if Lindsay had clarified the relationship between the book's stated dependent variable (information practice) and its unstated dependent variable of victory in battle." I agree that it would have been helpful, and I often asked myself many of the same questions. I ultimately made the decision to sacrifice some precision for the sake of readability, lest the theoretical explanation become as complex as the things it sought to explain. I gesture towards the complex relationships between technology, practice, innovation, and performance early on (33 Fig 2.1), but Biddle is absolutely right that much work remains to be done to clarify and test these relationships. My focus on information problems, solutions, and practice can thus be understood as a deliberate attempt to balance the inherent tensions, which may ultimately be irreconcilable, between Dunn Cavelty's call for greater attention to interpretive "co-production" with Biddle's call for clearer specification of causal mechanisms.

To complicate the problem even further, information practice—the ongoing organizational effort to adapt and repair the sociotechnical systems that enable knowledge and control—matters at the tactical, operational, strategic, and political levels, often manifesting in different patterns at each level, and often spanning different organizations and nations. This makes the correlates of informational performance and organizational performance very difficult to disentangle. All other potential determinants of military performance (civil-military relations, firepower, logistics, training, strategy, morale, etc.) cast an informational shadow and require information for their operation. Information practice is thus ubiquitous, and indeed necessary for performance of any kind. Yet the quality of information practice is insufficient on its own for explaining military effectiveness, precisely because it is an intervening variable that describes intermediating systems. This is why I stress that "Supplementary theory is needed in any particular case to explain why" (70) information problems and solutions take the form that they do. One implication is that I expect battlefield failures, for whatever reasons, to be strongly correlated with information frictions, precisely because most of the other determinants of military effectiveness also shape information problems and solutions. Yet this also means that it is possible for a military to experience something like victory despite serious information problems, especially if the enemy is even unluckier in this regard. The one thing that I can say with more confidence is that if militaries rely more on information technology in their operations, then information practice will be a more important factor in determining their battlefield effectiveness.

I am especially grateful for Cronin's close engagement with the text and positive feedback, particularly on the ethnographic chapters (4 and 5). She also raises a few "minor quibbles" that, as above, underscore the challenges of generalizing for a diverse audience. Cronin is correct to point out that "the term Revolution in Military Affairs (or RMA) is used loosely throughout." The term emerged in a specific milieu in the 1990s, to be sure, but key ideas were anticipated decades earlier and recapitulated decades later. The RMA episode just happens to be the most exaggerated expression of what I call "the technology theory of victory"(13) to emerge to date, even as it was never really implemented, and indeed never could be implemented, by even its most earnest proponents. The RMA ideology was always a caricature of itself, even as it gestured at important historical changes in the complexity and technological mediation of military power. I thus employed the term as a useful trope or synecdoche for highlighting the ever-present risks of deterministic thinking, whatever the actual information technology involved.

Cronin likewise questions my anachronistic references to Clausewitz, who inspires conflicting emotions in the security studies community ranging from adulation to scorn. Here Cronin and I seem to have different interpretations of the relevance of the Prussian theorist for understanding modern military organizations. As Cronin rightly points out, the Clausewitzian "paradoxical trinity" does speak to "competition between *societies*," but Clausewitz also, and earlier, defines war as "nothing but a duel on a larger scale."[33] Most of *On War* is a discussion of routines, frictions, tactics, and planning within the military organizations that actually fight these large-scale duels; Clausewitz writes far less about actual politics and social relations. Yet even more germane to my project, I believe that some of the enduring appeal of Clausewitz to military professionals comes from his ethnographic sensibilities. Clausewitz was an insightful participant-observer of warfare during an era of revolutionary change. His text continually highlights the frictions and uncertainties afflicting actual military

[33] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 75.

practice in his day, as well as their contrast to so much contemporary strategic theory. This example inspired me similarly to look beyond the technologist rhetoric at the actual information practice that is so often at odds with it. As with the RMA, I might be fairly accused of taking Clausewitz out of historical context, but I believe that both help to illuminate historical continuities in the nature of war (and naïve claims about war) that transcend the vintage of tactics and technology.

All the reviewers comment favorably on the ethnographic detail of the central case studies in the book. I confess this was something of a relief for me. Ethnography is a risky methodology. It delves into the granular, particularistic details of relatively minor cases, often leveraging the researcher's accidental circumstances, yet most scholars value generalizability and replicability. Ethnography also lends itself naturally to constructivist interpretations and epistemologies, yet mainstream security studies has a more positivist and realist orientation. More problematically, the ethnographer can hardly eliminate personal bias in the collection and interpretation of data. I was surprised that no one asked explicitly whether my optimism about user innovation in the FalconView case (ch 4) or my pessimism about Naval Special Warfare in the Iraq case (ch 5) had anything to do with my own organizational interests while in uniform, in the former case as an amateur developer of FalconView extensions, or in the latter case as a subordinate "tech" staff officer responsible for "indirect action" within a dominant "operator" culture focused on "direct action." Since bias cannot be eliminated, ethnography seeks to turn it into an asset, not only to gain access to study communities, but more importantly as an opportunity for self-conscious reflection on the role of bias in the construction and maintenance of social reality. Embracing one's own bias, ironically enough, can help to surface the very tensions and conceptual alternatives that provide raw material for a more generalizable explanatory theory.

As I explain in the book's appendix, which Dunn Cavelty gently chides me for not showcasing more prominently in the main text, this interpretive process makes ethnography an excellent methodology for theory construction. Yet as Biddle's insightful questions suggest, it may not be equally well suited for rigorous analytical testing, which is better accomplished via controlled case comparison or econometric methods. Ethnographic validity, rather, is established through a somewhat different process, a sort of folk Bayesian updating, whereby other participant-observers, with similar access to similar situations, recognize something of their own experience in the way general patterns have been articulated. Biddle implicitly describes this process, reflecting on his own experience in the field, when he kindly writes that my "theoretical analysis explained, far better than any other account I've read, not just what I saw in other headquarters, but why, and why these organizations produced the results they did in their efforts to understand their environments." Ethnography can be a risky bet, and I would not recommend it to many students, but apparently it pays off in some situations.

This response has already gone on too long, even as there is much more that could be said. Writing a book can be a lonely endeavor, but brief moments of community like this roundtable make it all seem worthwhile. I am deeply grateful to all the reviewers for taking the time to read my work and provide such thoughtful and generous comments. I am still painfully aware of many flaws and shortcomings in the book, many of which the reviewers were kind enough to leave unmentioned, but I am humbled and gladdened that they found something worthwhile. I am especially encouraged by the positive reception given to interdisciplinary work addressing practical problems, and I hope that this example might motivate others to question the limits of disciplinary and methodological boundaries. Personally, I am newly motivated to keep exploring some of the issues and questions that the reviewers raise, for this book has only scratched the surface of information technology and military power. Most of all, I am excited to see how these conversations will develop, with all the inevitable friction and adaptation that implies.