H-**Diplo** | **ISSF** Roundtable XII-14

issforum.org

Audrey Kurth Cronin. ***Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists.*** New York: Oxford University Press, 2020 [2019]. ISBN: 9780190882143 (hardcover, $29.95).

26 July 2021 | https://issforum.org/to/ir12-14
Editor: Diane Labrosse | Commissioning Editor: Michael Neagle | Production Editor: George Fujii

Contents

Introduction by Randall D. Law, Birmingham-Southern College

Audrey Kurth Cronin's new monograph, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, makes a valuable contribution to the literature on terrorism, technological innovation, and the evolving nature of national security in the twenty-first century. The book deserves to be widely read by scholars and policymakers. Deborah Avant, Boyd P. Brown III, and Jennifer Spindel have supplied us with insightful reviews that interrogate, respectively, the book's theoretical framework, its historical underpinnings, and its policy implications. Cronin's response helpfully answers some of her reviewers' questions and acknowledges where more work is to be done. In my introduction to this roundtable, I do not wish to recapitulate either Cronin's or her reviewers' arguments, since they all speak quite ably for themselves. What I do want to do is take a step back and try to illuminate some of the broader issues at play. In short, what does *Power to the People* tell us about the state of terrorism studies in 2021?

I find *Power to the People* significant for three distinct reasons. I am excited by its refreshing attitude toward the relationship between ideology, strategy, tactics, and technology and its author's eagerness to share her sources. I am also taken with Cronin's genuinely interdisciplinary approach, but on this count my enthusiasm is tempered by some lingering concerns that I have for the entire field.

Power to the People is – to my thinking – the best widely available work yet written on the relationship between terrorism and technology in large part because it adopts the clearest and most sophisticated framework so far developed. Cronin highlights several earlier works on this relationship; they have collectively served the field well by surveying the myriad ways in which the development of new technologies – particularly regarding weapons, logistics, and media – have led to the wider use of terrorism or its evolution as a strategy. But most of these earlier scholars have emphasized the trickle-down effect of new battlefield weapons. Cronin looks elsewhere. Here I would like to make note of one book that Cronin only briefly mentions and that stands in many ways as the most important predecessor to Cronin's book: Ann Larabee's 2015 *The Wrong Hands: Popular Weapons Manuals and Their Historic Challenges to a Democratic Society*.[1] Larabee explores the critically important idea that many weapons favored by terrorists – such as dynamite – began as technologies that were designed to benefit humanity and then spread via open-source handbooks that make them readily available to those with violent agendas. In the end, Larabee's book largely concentrates on the implications for free speech and even democracy of the tug-of-war between those who would limit and those who would champion the availability of these new technologies. Cronin develops the broader implications for terrorism by conceptualizing terrorists' favorite new weapons – again dynamite, but also the AK-47, and a host of other weapons – as those that began as disruptive technologies emerging as part of "open" technological revolutions. Thus, it is not simply the viability or use of the weapons that spread terrorism, transform terrorist strategies, and pose the biggest threats to society; rather it is the social changes occasioned by the disruptive, open-source nature of the technologies that transform how terrorism becomes more viable, impactful, and attractive. This insight helps explain why certain technologies do more to spread terrorism, transform terrorist strategies, and pose the biggest threats to society. And this explanation makes abundantly clear why artificial intelligence, 3D printers, drones, etc., are the twenty-first century equivalents of dynamite in both their promise and their peril.

I will touch only briefly on a second way in which I find *Power to the People* to be so significant, and that is Cronin's sharing of sources. The field of terrorism studies has long benefited from the development of open-source databases, the most important of which has been the Global Terrorism Database,[2] which was developed at the University of Maryland under the auspices of the National Consortium for the Study of Terrorism and Responses to Terrorism (START). What Cronin has

[1] Ann Larabee, *The Wrong Hands: Popular Weapons Manuals and Their Historic Challenges to a Democratic Society* (Oxford: Oxford University Press, 2015).

[2] The National Consortium for the Study of Terrorism and Responses to Terrorism (START), "The Global Terrorism Database (GTD)," https://www.start.umd.edu/gtd.

done, though, is to immediately share on her personal webpage[3] several databases on the development and spread of weapons technologies that she and her team built explicitly to write this book. I hope that Cronin's example of communal scholarly striving will encourage others in the field of terrorism studies to likewise share not just bibliographies and results but the actual data, thus jumpstarting more research, particularly that of junior scholars.

Finally, *Power to the People* is a striking example of the breakthroughs that can be achieved by scholars who work outside of what often feels like hermetically sealed disciplinary categories. I say this as a well-established and practicing historian of terrorism: very rarely have we been presented with a data-driven work on terrorism that makes such impressive use of historical sources and a compelling historical framework. The result is a book that reveals meaning like the layers of an onion – a book that can be equally appreciated, endorsed, and exploited by historians, social scientists, and policy experts.

I do not offer this praise lightly. Those who work in the field of "terrorism studies" know all too well the opportunities and perils that exist for those who try to work these interstitial spaces. "Terrorism studies" emerged in the 1970s and 1980s in response to the need for experts to make sense of the increased use of terrorism by anti-colonial and radical left movements during the post-war era. Most terrorism experts came out of political science, in large part because the critical demand for policy and military solutions led to an overwhelmingly presentist orientation and thus a quantitative, model-driven, extrapolative framework. Some experts on terrorism emerged in the fields of philosophy, economics, psychology, sociology, and communication studies, but more often than not these experts talked past each other, unable or unwilling to speak each other's languages. For a long time, the most glaring problem was the difficulty with which historical insights were incorporated into the field. Given its longitudinal view and the sheer wealth of human experience with terrorism, the field of history is an indispensable contributor. But as one of the most Balkanized and conservative disciplines, history has often been its own worst enemy, achieving only mixed results in speaking beyond the ranks of its own practitioners until fairly recently. All too often works on terrorism – whether introductions to the topic at large or narrow explorations of specific aspects – begin with a brief historical survey that makes overly broad generalizations that yield few actionable insights. The 9/11 attacks worsened the problem by producing an anxious, desperate populace that lapped up the 'analysis' – by turns simplistic, sensationalistic, or simply wrong-headed – that was eagerly churned out by a burgeoning terrorism-expert industry. In short: hard-working members of the terrorism studies community learned to duck and cover whenever a shallow expert glibly invoked 'the lessons of history.'

Enter Cronin's book. Her incorporation of detailed explorations of the rapid proliferation of Alfred Nobel's dynamite and Timofey Kalashnikov's AK-47 into her broader argument is sophisticated. Each case study is thoroughly grounded in nuanced descriptions of the historical eras that produced these innovations, descriptions that necessarily spill over into evocative analyses of many adjacent topics. This is well-executed historical methodology in service of a very specific, practical research question, one that is executed to yield specific insights into how to curb the proliferation of "disruptive technologies" that undermine security, stability, and democracy today.

My one caveat is to note with some chagrin that Cronin's book relies on the political scientist David Rapoport's "Four Waves" model of terrorism that posits that terrorism has developed in four stages: anarchist "propaganda of the deed" in the nineteenth century, anti-colonial wars of independence in the mid-twentieth century, the recrudescence of radical leftist violence in the 1960s and '70s, and the rise or fundamentalist religious violence since the 1980s.[4] There is much to recommend Rapoport's analysis, particularly his emphasis on how the use of terrorism evolved out of intertwining ideological, social, strategic, and technological factors. The problem with the "Four Wave" approach, as it always is for historians encountering a social scientific model, is what it leaves out. And what is left out in this case completely upends

[3] Audrey Kurth Cronin (website), https://www.audreykurthcronin.com/.

[4] Rapoport first presented a full version of his model in response to the 9/11 attacks: Rapoport, "The Fourth Wave: September 11 in the History of Terrorism. *Current History* 100:650 (2001): 419–424. He later revised the model several times; the last version can be found at Rapoport, "The Four Waves of Modern Terrorism," 41-60, in John C. Horgan and Kurt Braddock, eds., *Terrorism Studies: A Reader*, eds. John C. Horgan and Kurt Braddock (Abingdon: Routledge, 2011 [2008]).

our fundamental understanding of terrorism. Rapoport's approach barely acknowledges the origins of modern terrorism in the French Revolution and the early-nineteenth century development of the surveillance state based on the chimera of sub-state terrorism. The significance of this is the continuing insistence by many terrorism scholars that terrorism is definitionally carried out by sub-state entities and is generally reducible to a strategy without acknowledging the post-structural nature of terrorism – at least in some instances – as a construct. Moreover, the Four Wave model completely ignores the largest nineteenth-century terrorist campaign, that of the Ku Klux Klan, white supremacists, and government officials (via Jim Crow and lynching) in the decades after the American Civil War. *Power to the People*'s framework doesn't really depend on the Four Wave model for its insights, which makes its invoking of the model all the more regrettable.

This quibble aside, *Power to the People* is a brilliantly conceived and executed book, one that terrorism studies experts can look to both for its specific insights and signal achievements in conceptualizing the role of technology, furthering collegial research, and making use of an authentic interdisciplinary approach. Kudos to Cronin.

Participants:

Audrey Kurth Cronin is Distinguished Professor of International Security at American University in Washington, DC, and founding director of the Center for Security, Innovation, and New Technology. 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, cyberphysical systems, synthetic biology, autonomy, and artificial intelligence, especially their use by terrorists, insurgents, proxy armies, and other private actors. *Power to the People* was named one of *Foreign Affairs*' "Best of 2019," was a finalist for the 2020 Lionel Gelber prize, and won the 2019/2020 Neave Book Prize for "the most significant, original, relevant, and practically valuable contribution to the understanding of terrorism."

Randall D. Law is Professor of History at Birmingham-Southern College in Birmingham, AL, where he teaches courses on Russia, modern Europe, and the history of terrorism. He is the author of *Terrorism: A History*, 2nd, ed. (Polity, 2016) and the editor of *The Routledge History of Terrorism* (Routledge, 2015).

Deborah Avant is Professor, Sié Chéou-Kang Chair, and Director of the Sié Chéou-Kang Center for International Security and Diplomacy at the Josef Korbel School of International Studies, University of Denver. Her research (funded by the John D. and Catherine T. MacArthur Foundation, the Smith Richardson Foundation, and the Carnegie Corporation, among many others) focuses on the politics of managing violence and generating governance at local, national, and global levels. Professor Avant was the founding editor-in-chief of the International Studies Association's *Journal of Global Security Studies*. She is author/editor of *Civil Action and the Dynamics of Violence in Conflicts* (with Sié Center colleagues); *The New Power Politics: Networks and Transnational Security Governance* (with Oliver Westerwinter); *Who Governs the Globe?* (with Martha Finnemore and Susan Sell), *The Market for Force: the Consequences of Privatizing Security*; and *Political Institutions and Military Change: Lessons From Peripheral Wars*, as well as articles in such journals as *International Organization*, *International Studies Quarterly*, *Security Studies*, *Perspectives on Politics*, *International Studies Review*, and *Foreign Policy*. She is now writing a book and several articles on pragmatic approaches to global governance.

Boyd Brown III is an Associate Professor of Criminal Justice at Nichols College in Dudley, Mass., where he has taught since 2012. He has a bachelor's degree in History and Anthropology from the University of Maine, a master's degree in Biological Anthropology from the Ohio State University, and an Advanced Certificate in Terrorism Studies from John Jay College of Criminal Justice. His research interests include the militarization of the police, wrongful convictions, and Middle Eastern/African terrorism.

Jennifer Spindel is an Assistant Professor of political science at the University of New Hampshire. She is working on a book manuscript about signaling in international politics and the conventional weapons trade. Her research has appeared in *Security Studies*, *Armed Forces & Society*, and the *Journal of Global Security Studies*.

Review by Deborah Avant, University of Denver

Audrey Cronin has written a smart book. She orients her argument around the difference between 'closed' (highly controlled by states) military technological innovations like nuclear weapons and 'open' (uncontrolled and widely dispersed to many outside of states) innovations like dynamite. She traces the impact of open innovations in recent history, including dynamite and KalashnikovAK-47s. After examining the innovative potential and diffusion of these weapons, she turns to how they have built on one another and have been vastly aided by the current open technological innovations which are the central focus of the book. She describes a staggering array of risks this poses and calls for democracies to regulate these innovations more thoroughly and to prepare to defend against the coming anarchist threats.

There is much to like about this book. It is well written and well researched. I learned a great deal about both dynamite and Kalashnikovs. Her description of the way current innovations could go wrong is also thorough and often well-founded. There is a handy methodology section at the end, with descriptions of her sources and data. I wondered about why the book discusses these two innovations and not others – say other types of small arms – but this is merely a quibble.

I was less persuaded by the theory of lethal empowerment. The logic of the book focuses on an order/anarchy binary, implicitly assuming that state power is most likely to manage violence in a beneficial way. This causes her to ignore the fact that technology also changes and enables malevolent *state* action. Furthermore, the same features that point to lethal empowerment also empower non-lethal, even beneficial action, whether through connecting climate change activists or providing tools for innovative apps to contain the COVID-19 pandemic. If regulation does not take account of what is necessary for continued innovation, it could backfire by impeding beneficial action. Finally, states have not been the only 'governors' of technology. Indeed, Laura DeNardis claims that the very definition of Internet governance is "distributed and networked multistakeholder governance, involving traditional public authorities and international agreements, new institutions, and information governance functions enacted via private ordering and arrangements of technical architecture."[1] These promising governance techniques that aim to mitigate malevolent action by states and nonstate actors alike should not be ignored. So, while I appreciate Cronin's examination of the historical cases, I find the analysis of what they mean and what we should do about our current challenges less useful.

Cronin addresses her argument to states, particularly the U.S. and the other 'democracies' it often joins with, along with the military and intelligence organizations that carry out national security (as it is traditionally imagined). As we have seen, though, particularly over the last four years, the contemporary technical revolution has altered these very entities. Indeed, we could think of Cambridge Analytica's impact through the prism of what Cronin calls the "hijacking of psychological tactics" (197). Rather than enabling non-state 'terrorists,' it has permitted the undermining of elections around the world. Social media has also allowed some global leaders to amplify falsehoods and spread disinformation even in (admittedly declining) democracies like the United States. And, for even longer, drone technology has allowed a kind of targeted killing that many observers have deemed counter to international humanitarian law.[2] Looking to the U.S. and other 'democratic' states as the purveyor of order and protection against malevolence has been put to question.[3]

[1] Laura DeNardis. *The Global War for Internet Governance* (New Haven: Yale University Press, 2014), 23.

[2] For instance, Human Right Watch's letter to President Obama in 2010, https://www.hrw.org/news/2010/12/07/letter-obama-targeted-killings-and-drones.

[3] Of course, this caution holds for the past as well. See Robert Vitalis, *White World Order, Black Power Politics: The Birth of American International Relations* (Ithaca: Cornell University Press, 2015). And it holds for governments other than the United States. See Alexander Aneivas, Nivi Manchanda, and Robbie Shilliam, *Race and Racism in International Relations: Confronting the Global Colour Line* (New York: Routledge, 2015).

The theory of lethal empowerment Cronin builds draws from Clayton M. Christensen's conception of disruptive innovations.[4] But almost all the criteria by which something is subject to lethal empowerment, including (but not limited to) low cost, ease of use, multiple uses, transportability, symbolic resonance, are also those that allow for innovation and beneficial use. Cronin argues much later in the book, and I agree, that regulation is not strangulation (265). But how to regulate without strangling is not straightforward – especially when, as she admits, policymakers are sorely lacking in technical proficiency (266). It often requires re-thinking how an organization, be it the U.S. government or parts of the U.S. military, operates. It may include, as Jacqueline Schneider puts it, allowing "blue hair in the grey zone" and other cultural and physical reconsiderations of what a warrior is like.[5] It also may include revisiting what is ethical for warriors to do.[6] Given the second and third order effects of problematic regulation – including pushing would-be good citizens into illegal action because they question the legitimacy of what their government is asking them to do (witness whistleblower and leaker Edward Snowden) – noting that regulation is not strangulation is not enough. There needs to be consideration of how regulation could work in this new, and swiftly changing, environment.

This brings me to my final point. Cronin mentions, both in the introduction and the conclusion, the potential responsibilities of technology companies, but her focus is on state regulation as a means to get them under control. Unmentioned is the work of multi-stakeholder organizations like the Global Network Initiative that have engaged companies, civil society organizations, and academic experts to work toward initiatives to limit internet-enabled repressive and violent actions no matter who is carrying them out. Similarly, Citizen Lab, at the University of Toronto, has aimed its reporting on the use of technology to undermine rights. While there is a mountain of evidence that state regulation is important, it is also clear that states can be captured by narrow interests.[7] The likelihood of productive state action is often improved when businesses and civil society groups also commit to public-oriented action. Engaging with these various organizations can be an avenue to productive new frames for mitigating the use of violence.[8] This does not mean ignoring more traditional ideas about national security, but it does push these ideas to take account of global interdependence in ways that limit, rather than enhance, the prospects of weaponizing it.[9]

In sum, this is a smart and important book. We can learn a lot about the way the more open system of innovation can diffuse and be used for violent purposes by looking at past open systems of warfare innovation. As is becoming increasingly clear, though, information technology is not simply a tool. It interacts with and through human beings, and is changing human behavior.[10] Thinking about how to manage the malevolence it promises should lead us to think more broadly and critically about states as well as non-state actors, to contemplate the double-edged nature of many technological features that

[4] Clayton Christensen *The Innovator's Dilemma* (New York: HarperBusiness, 2011).

[5] Jacqueline Schneider, "Blue Hair in the Grey Zone." *War on the Rocks* (blog), 10 January 2018, https://warontherocks.com/2018/01/blue-hair-gray-zone/

[6] For an example of this thinking, see, for instance, Daniel R. Brunstetter and Jean-Vincent Holeindre, eds., *The Ethics of War and Peace Revisited: Moral Challenges in an Era of Contested and Fragmented Sovereignty* (Washington, D.C.: Georgetown University Press, 2017).

[7] See, for instance, Walter Mattli and Ngaire Woods, "In Whose Benefit? Explaining Regulatory Change in Global Politics" in Walter Mattli and Ngaire Woods, eds., *The Politics of Global Regulation* (Princeton: Princeton University Press, 2009).

[8] See, for instance, efforts to regulate the private military and security industry. Deborah Avant, "Pragmatic Networks and Global Governance: Explaining Governance Gains in Private Military and Security Services," *International Studies Quarterly* 60:2 (2016): 330-342.

[9] Henry Farrell and Abraham Newman, "Weaponized Interdependence," *International Security* 44:1 (2019): 42-79.

[10] Ronald J. Deibert, *Reset: Reclaiming the Internet for Civil Society* (Toronto: Anansi, 2020).

challenges simplistic regulatory fixes, and to engage in a much broader public sphere about how to think about national security in ways that respects productive interdependence and limit attempts to weaponize it in the service of opportunistic individuals and groups.

Review by Boyd P. Brown III, Nichols College

In 2017, at the annual Global Security Expo in Las Vegas, Scott Klososky, the founder of Tri-Corps Technologies, gave a presentation titled "*Security in a Transforming Digital World*," in which he discussed the perils of living in an increasingly VUCA (Volatile, Uncertain, Complex, Ambiguous) world. He used the lowly tollbooth to illustrate our reliance on, and the spread of, more advanced technology. Barely a hundred years ago, tollbooths were staffed by humans and each car had to stop to pay their fee. By the end of the century, technology had taken over so that humans were replaced by automated "coin catchers" with a gate. By early in the twenty-first century, even that technology had been supplanted by automation that completely removed the human from the equation and, through such innovations as the 'Easy Pass,' does not even require the driver to stop.[1]

In *Power to the People*, Audrey Kurth Cronin masterfully continues this conversation and narrows the focus to how the ease of access to disruptive technology presents a growing, global, security threat. Cronin's analysis is ultimately about the law of unintended consequences. As she points out in her introduction, "Innovation is undoubtedly the engine that drives human progress … but every technological innovation involves risks as well as promises. … The focus here is on technologies that were developed with good intentions, such as digital media and drones" (5). She uses historical examples and modern trends to illustrate the under-appreciated challenge not only that emerging technologies present, but also the arenas from which they emerge. Cronin charts the link between military conflict and innovation and argues there is an intimate link between the two. She points out that initially innovation was initially seen as a threat because "manufactured products left craft workers behind, and the cultural changes ushered in led to horrible working conditions for many, as well as … political revolutions that destabilized governments and killed millions in revolutionary wars" (28). Over time, however, innovation was increasingly seen as decisive on the battlefield and, along with it, an assumption was made that individual technologies could provide significant advantage to the side the wielded it. She also frames her book within "lethal empowerment theory," which she describes as "helping to anticipate which new technologies hold the greatest potential to become popular tools for political violence in the future" (13).

Cronin takes a semi-chronological approach, and her book is divided into three main sections. In the first, she introduces theories on open and closed technological innovation, and the diffusion of technology among nation-states. She then explains how insurgents, terrorists, and other non-state actors use innovation to their advantage. In this discussion, she uses David Rappaport's "four waves of modern terrorism" model and links it to significant trends in innovation and technological diffusion.[2] The first of these waves is represented by anarchist violence in the late-nineteenth century, followed by anti-colonial movements of the early-twentieth century. In the 1960s, a third wave began, defined by Marxist/Leninist struggles around the world and, finally, at the end of the twentieth century, the fourth wave of religious extremism grew in prominence. The waves can be identified not only by the ideologies that drove them, but also the technology that made violence possible, from dynamite in the first wave to mobile digital technology and suicide attackers in the fourth. While terrorism itself has received ample study, Cronin distinguishes her study because, as she points out "most terrorism scholars don't focus on the technologies used … they tend to focus primarily on *software* – ideologies, group strategies, organizational structures, decision-making processes, and leadership – and very little on the hardware" (47).

The hardware is the emphasis of the second section of the book, where she uses two historic examples, dynamite and the AK-47, to explore the consequences of closed versus open technological innovation. She argues that "during a closed revolution, social, political, or economic forces restrict access to emerging technologies. … By contrast, during an open revolution, emerging technologies are accessible to the public, and individuals and private groups are free to not only buy,

[1] Steven Klososky, "Security in a Transforming Digital World," given at the Global Security Expo on September 2018 held in Las Vegas, Nevada.

[2] David C. Rapoport, "The Four Waves of Modern Terrorism," in *Terrorism Studies: A Reader*, eds. John Horgan and Kurt Braddock (Abingdon: Routledge, 2008), 43.

use, and distribute them, but also to invent a new purpose for them" (19). Cronin's focus on closed versus open technological revolutions is crucial because, historically, military technology has tended to develop in a closed system, limiting its diffusion to non-state actors, insurgents, and terrorists. However, in her view, we have entered a stage of unprecedented open innovation that has the potential to undermine the established global order and change the very nature of warfare.

Dynamite serves as the first example of an open technology that diffused with unintended consequences. Cronin chronicles Alfred Nobel's desire to produce an explosive that was both safer and more powerful than the day's other explosives, gunpowder, and nitroglycerin. He intended his invention not for military means, but to help drive the engine of industrialization and progress. It certainly was not his intention that his creation would spur the first wave of modern terrorism. Dynamite was not seen as a useful weapon for the military, and in this way, terrorists were able to outpace the military in the use of dynamite in small, lethal, explosive devices. As Cronin points out, "The military priority was on long-range artillery and dynamite was found to be too shattering and unstable for that purpose" (98). However, for a myriad of organizations – among them Russia's *Narodnaya Volya*, Irelands' *Clan na Gael*, the international Anarchist movement, and several others that Cronin mentions – dynamite became the perfect force multiplier, and they began to innovate new and lethal methods to employ it.

The discussion of dynamite is thorough and eye-opening without being overly technical. Cronin documents how Nobel's invention quickly let the proverbial genie out of the bottle. Despite Nobel's efforts to control the production and sale of his product, both through patents and the construction of manufacturing plants around the world, dynamite quickly proliferated. One of the primary reasons dynamite diffused so far and wide was because of how frequently it was copied. "As word of dynamite spread, dozens of knockoff products that mixed nitroglycerine with other stabilizers quickly emerged…indeed there were as many as 125 different dynamite varieties…" (99-100). This was coupled with a reluctance of governments to restrict or regulate the explosive due to its popularity within industry, particularly railroads and mining. This pattern held even after a wave of accidents and attacks highlighted the dangers from the new explosive. As Cronin observes, dynamite serves a powerful example of the unintended consequences of new technology because when a new, profitable technology is introduced, "it can be difficult to control its spread, especially if the new technology is commercially produced, has positive uses, and stands to make many people lots of money" (123).

The discussion of the development, diffusion, and disruption of the AK-47 is just as deftly handled. Cronin chronicles the development of the weapon in the context of World War II. She points out that the Soviet leaders initially kept the weapon a very closely guarded secret, mostly due to Soviet Premier Joseph Stalin's belief that it gave the Soviet military a distinct advantage over its adversaries. In this way, it was a closed technological innovation and, consequently, its diffusion was quite limited. Although the weapon was adopted in 1948, the Soviets did not share it with their allies. For example, while the Soviet Union helped to arm the North Korean army during the Korean Conflict, they did not allow the AK-47 to be exported; that occurred only during the Hungarian uprising in 1956. Ironically, it was a photo of an insurgent, rather than a Soviet soldier, armed with the weapon, that made its way into newspapers around the globe.

Stalin's successor, Nikita Khrushchev, used the AK-47 as both leverage to improve relations between the USSR and its allies, but also because of its economic value. Cronin argues that "While the ruble had no value outside the USSR, Kalashnikovs certainly did, and they became a form of global Soviet currency, especially precious while the USSR was still the primary producer" (147). In a few short years, the AK-47, and its variants, were being produced in China, Egypt, Poland, East Germany, and many other Soviet-allied countries. Other states, such as Yugoslavia, simply reverse engineered the weapon and began to produce it on their own.

This is yet another point in her book where Cronin deftly handles a complex topic. She shifts her focus from a broad historical narrative to explore the consequences of the AK-47 and its diffusion. To make her argument, she references the Correlates of War Project. This study, "found a sizeable uptick in the defeat of state forces: between 1900 and 1949, rebels won 34.9 percent of the time, while after 1950, that rose to 55 percent" (161). While cautioning the reader that the Kalashnikov is not the only reason for this trend, Cronin observes that "the growing worldwide availability of Kalashnikovs seems to be an important element, one that is commonly overlooked in both academic and policy studies of civil war,

insurgency, and terrorism" (162). Just as importantly, however, is how, as with dynamite, Cronin identifies the unintended consequences of the weapon, specifically, the number of conflicts in which it has been turned against the very regimes that produced it, often with destabilizing effects.

The core of *Power to the People* is the section dedicated to dynamite and the Kalashnikov. Cronin uses these historic examples to frame her argument about the risk posed by our current, mostly open, age of technological innovation. The book's step into the twenty-first century explores diverse technologies such as drones, self-driving cars, facial recognition software, and smart phones. Cronin argues that with these, and a myriad of other technologies, we have entered an age of unprecedented open technological innovation. In many regards, this age is not all that different from the ones that came before. Like dynamite, these new innovations have been used in novel and destabilizing ways, such as the 2011 attempt by Rezwan Ferdaus a man from Massachusetts to use a remote-controlled plane to bomb the Pentagon, or the 2019 attack by Iranian backed Houthi rebels that successfully targeted the Aramco oil facility in Saudi Arabia using explosive laden drones.[3]

What distinguishes the current era of open innovation is the way in which it is facilitated by the Internet of Things. While both dynamite and the Kalashnikov benefitted from emerging communication technology of their day, in the form of newspapers and network news respectively, the Internet of Things provides unparalleled access to hobbyists, tinkerers, and those who would seek to do harm by using emerging technology. "The maker movement, which celebrates hands-on creativity by hobbyists of all types, along with community labs like hackerspaces, where amateurs can access technology tools and share ideas, are thriving" (259). This, according to Cronin, creates a unique threat environment that allows for the rapid sharing of ideas, expertise, and new innovations. To illustrate the new threat landscape, Cronin documents a host of recent examples and hypothetical situations. She starts with the story of a group of students from the University of Virginia who used 3-D printing technology to produce a drone that they then coupled with an Android phone's navigation system to allow it to fly "without line-of-sight radio contact or an expensive navigation system. … A slick YouTube video shared the results of their experiment worldwide … the simple design accommodated printing the drone smaller or larger to make it suitable for carrying anything from mail to an explosive, all in about thirty hours for less than $2500" (200). Cronin also highlights how multiple insurgent groups, including Hezbollah, Hamas, and (work in full name) ISIS have either used readily available hobbyist drones or started their own drone programs. She discusses how ISIS was able to exploit social media to recruit more than 40,000 members worldwide and then use that same social media as a force multiplier to instill fear in their adversaries, most notably the Iraqi soldiers who were defending Mosul, to break their will to fight.

Cronin posits a growth of "new feudalism," in which consumers own their own devices, but the applications and tools that make that device run – that is, the means of production – are owned and controlled by some distant, anonymous corporation, making the consumer dependent on a digital "company store." She warns of cars that now harvest gigabytes of data on the habits and history of the driver and transmit that data to "third party venders, many with dubious security protections" (264). She sees a near future in which remotely controlled or hacked vehicles, swarms of drones with facial recognition software, or a myriad of other technologies are hacked, manipulated, or adapted by non-state actors to wreak havoc, destabilize established regimes, and usher in a new era of "propaganda of the deed."

The book's final section is a warning to the West. Cronin points out that, with the exception of a few of the Scandinavian and Baltic states that border Russia and have developed robust systems to protect their digital infrastructure, most other countries lag far behind. Cronin's analysis suggests that if the United States and Western Europe do not confront this threat rapidly and aggressively, the consequences could be dire. *Power to the People* is an important study that offers insights to the

[3] Carol Cratty and Michael Martinez, "Man, 26, Charged in Plot to Bomb Pentagon using Model Airplane." *CNN*, September 29, 2011, last accessed November 20, 2020, https://www.cnn.com/2011/09/28/us/massachusetts-pentagon-plot-arrest/index.html; Ben Hubbard, Palko Karasz, and Stanley Reed, "Two Major Saudi Oil Installations Hit by Drone Strike, and US Blames Iran." *New York Times*, September 14, 2019, last accessed November 20, 2020, https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html.

VUCA world of the twenty-first century. It is a valuable read for any historian, technology expert, or security professional who is interested in the dynamic nature of our new reality.

Review by Jennifer Spindel, University of New Hampshire

Power to the People tackles two issues of increasing political relevance. First, it seeks to explain the birth of modern terrorism by referencing previous moments of violence, and second to show how military diffusion and the diffusion of technology work for non-state groups. To accomplish the first goal, Cronin undertakes an expansive review of terrorism through her case studies. For the second, she develops a typology of technological revolutions. She argues that new technologies will be rapidly adopted and innovated with when they meet certain key criteria, including accessibility, low price point, and simplicity of use. Accessibility plays a large role in her explanation, and she develops the concepts of "closed" and "open" revolutions (19). In the former, access to emerging technology is restricted primarily to scientific or political elites, as was the case for radar, nuclear weapons, and battleships. Open revolutions occur when emerging technologies are accessible to the public, and individuals and private groups can use, distribute, and invent new purposes for that technology.

This book fills a number of important gaps in scholarship about technology and violent non-state actors. Cronin frequently references the unintended and unanticipated outcomes of technological innovation, a useful reminder that future implementations of a given device are often unpredictable and can have wide-ranging political effects. For example, she notes that the book focuses on technologies that were developed with good intentions, like digital media and drones, that were supposed to alleviate social problems or to minimize casualties in war. The book shows, however, how technologies have often shifted the locus of power from dominant players to "surprise actors" (8).

The book shares similar goals to work on the diffusion of military power, but shifts the focus to non-state actors.[1] Cronin provides new insights about how and why technology matters for international politics by focusing on non-state actors. In turn, the book also contributes to work on power asymmetries and war, and shows that innovations in low-tech solutions often explain why insurgent forces are able to stymie or defeat major militaries (53).

Cronin cautions her readers against assuming that certain technologies have inevitable strategic consequences. She notes that technology is not the same thing as strategy, nor does technology imply a particular strategy (31). Instead, most revolutionary changes in warfare have been the result of "broader changes in society affecting who used weaponry, where, why, and how" (3). It is those key questions – where, why, and how – that are the focus of the case studies in the book. This focus on how technology has been used, and the political and social context in which it was deployed, shifts her analysis away from reifying technologies or falling into the trap of assuming that certain technologies are offensive or defensive. As Colin Gray argues, "technology and its effective military application are dependent, not independent, variables."[2] Early on, Cronin notes the importance of holding on to political and social contexts, though this topic sometimes slips out of focus in later

[1] On the diffusion of military technology, see Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton: Princeton University Press, 2010); Michael C. Horowitz, "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism," *International Organization* (2010): 33–64; Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact from Fiction in the Debate over Drone Proliferation," *International Security* 41:2 (2016): 7–42; Andrea Gilli and Mauro Gilli, "The Diffusion of Drone Warfare? Industrial, Organizational, and Infrastructural Constraints," *Security Studies* 25:1 (2016): 50–84.

[2] Colin S. Gray, *Weapons Don't Make War: Policy, Strategy, and Military Technology* (Lawrence, KS: University Press of Kansas, 1993), 38. See also Bernard Brodie, "Technological Change, Strategic Doctrine, and Political Outcomes," in *Historical Dimensions of National Security Problems*, ed. Klaus Knorr (Lawrence, KS: University Press of Kansas, 1976), 263–304.

chapters. Nonetheless, highlighting that humans decide how to use technology is a useful way to skirt the offense-defense debate, and instead allows her to examine the accessibility and diffusion of key technologies.[3]

By focusing on history and people, rather than just on technologies, Cronin connects incidents of violence that have often been analyzed separately. She discusses the "contagion" effects of social media and the proliferation of "news" outlets that have allowed anyone with a smartphone and internet connection to become a producer (and consumer) of media (54). As she notes, with the click of a mouse information can be accessible to billions of people and can exist in perpetuity (185). She does an excellent job capturing the paradox of the internet and the diffusion of internet-connected technologies (ICTs): it is now possible "to engage electronically, and globally, in the full span of human activities, from spreading hope, love, and enlightenment, to inciting hate, abuse, and murder" (175). One consequence of the ubiquity of ICTs is that "surprising underdogs" are able to reach larger audiences (178). Cronin notes, however, that this is not new: actors like al Qaeda militant Anwar al-Awlaki used cassettes and CDs before moving over to Facebook and YouTube in the early 2000s. Digital social technologies, though, allowed savvy marketers like Awlaki to attract a much broader audience (173).

Cronin's study of new technologies raises a number of questions about the skills needed to navigate this new world, and the relationship between state and non-state actors. For example, social media gives any actor a global audience, but also exponentially increases the competition for that audience's attention. Just as most people don't become YouTube stars or TikTok trendsetters; the diffusion of ICTs could simply mean that there are more people speaking into the digital void.

What makes the jihadist messages Cronin traces so appealing? More generally, why do some messages inspire global movements, while others remain stuck in obscurity?

Cronin hints at the answer to this question when she reviews the four waves of terrorism (41-42). She notes that terrorism has been anarchist, ethno-nationalist/separatist, "New Left," and, most recently, religious and fundamentalist. Although this brief look at history is important for reminding readers that terrorism is not a new phenomenon, it leaves unanswered the question of why those ideologies took hold at those particular moments in time. Imagine, for example, if Italy's Red Brigades, as emblematic of the "New Left," had had access to Facebook. Surely, they would have engaged in similar activities as the Islamic State (ISIS) and al-Qaeda. Here it would be useful to return to one of Cronin's early insights about the importance of political and social context. Why is it that the language of terrorism today is narrated as religious fundamentalism? This is an important question, because Cronin notes that the spread of livestreamed attacks allows groups to tailor their own narrative of events (189). She also makes passing reference to acts of violence committed in the U.S., some of which are white nationalist rather than jihadist-inspired.[4] At times it feels as though the focus on jihadism distracts from more important generalizable insights about how groups narrate their purpose, and how those narratives resonate, or do not, with potential adherents or supporters. In other words, Cronin's real insights about the spread and diffusion of technologies, and how that is related to violence, sometimes seem to get distracted by a focus on jihadist terrorism, and sometimes leaves bigger questions unanswered.

Cronin notes that groups and movements often cohere around important symbols, and a remaining question concerns how these symbols have shifted in the digital age. For example, dynamite and the AK-47 were part of the vivid imagery that helped draw attention to and spread the message of their users (260). What happens, though, when technologies are ubiquitous? A terrorist holding up a smart phone is indistinguishable from billions of other smartphone users. Small drones

[3] Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and How Can We Measure It?," *International Security* 22:4 (1998): 44–82; Stephen Biddle, "Rebuilding the Foundations of Offense-Defense Theory," *The Journal of Politics* 63:3 (2001): 741–74.

[4] Jenny Gross, "Far-Right Groups Are Behind Most U.S. Terrorist Attacks, Report Finds," *The New York Times*, October 24, 2020, sec. U.S., https://www.nytimes.com/2020/10/24/us/domestic-terrorist-groups.html; Sean Spence, "Right-Wing Extremism: The New Wave of Global Terrorism," *The Conversation*, October 22, 2020, http://theconversation.com/right-wing-extremism-the-new-wave-of-global-terrorism-147975.

that might be used to conduct violence are available on the shelves of Walmart and Target. Although violence can now be live-streamed, what does it mean for symbols and imagery of war when those symbols and images are drawn primarily from the social domain? Are we living in a moment in time where violent non-state actors might have the power to change how people think about what it means to engage in 'war' or violence? Will future generations look back and associate the cellphone or live-streaming with war and violence? More generally, Cronin opens the door for future work to analyze when and how has the dominant conceptualization of war been changed by the technological innovations of non-state groups.

Throughout the book, Cronin shows how different technologies can empower surprise actors, which raises questions about who and what matters for international politics, and how scholars and policymakers can and should study the proliferation of violent non-state groups. First, private companies are rising in importance, though Cronin understandably does not devote as much attention to this. However, there are certain examples that show the importance of incorporating private actors into the analysis. A proliferation of medical devices, public utilities, and home devices that are connected to the internet mean that companies that produce these devices will be an important part of any conversation about security in the digital age. Not only are Microsoft and Facebook relevant because of the hardware and software they create, but companies like LG and Samsung must also be part of the conversation. Governance is no longer the sole domain of governments and international organizations.[5]

Second, the identity of the technology's creator now matters. For dynamite or the AK-47, once the technology was created, it could be used without further involvement of the creator. Alfred Nobel did not collect information on the groups that used dynamite in their terror attacks. That is no longer the case. Cronin describes drones that were created by the Chinese company DJI, which sent location data back to the manufacturer every time they were launched (215-216). The U.S. military stopped using these drones in 2017, but the example shows that the creator of the new technology can remain involved in its use long after the technology has diffused. It might now matter to terror groups where the technology was created. Do they risk sending data to China, or using a Western-made app or platform that might not get past the Great Firewall? The example of DJI can also open a discussion about access to data and information, and how ICTs can extend the reach of authoritarian regimes that are often more willing to collect and store data.

Finally, Cronin traces a change in the type of knowledge that matters. You don't need to be a software engineer, or to understand how the internet works in order to be an effective influencer. Awlaki spoke in American colloquialisms to increase his appeal to English-speaking audiences (173). Instead, users need to understand how to harness group dynamics on these platforms. The skills that organizations – whether state, non-state, or private – most need are often not the hard tech skills that students learn by studying computer science. The skills in demand are in the realm of social science and humanities: what type of media content is going to garner the most views and have the most staying power? And yet, there is a limit to how far you get without a tech background. When Cronin discusses automation and artificial intelligence, she notes that non-state actors are unlikely to have access to or to adopt full artificial intelligence, but that these groups are and will use autonomous and semi-autonomous systems. Non-state actors, then, are likely to exist in a goldilocks zone where they need a basic level of technological knowledge in order to upload content and engage with audiences, but will remain below the technological knowledge level of states and private companies that develop these tools and applications.

In terms of studying violent non-state groups, Cronin's analysis highlights the need for network analysis. In discussing how online conspiracy theories can incite 'lone wolf' attackers, Cronin hints at how digital and social technologies can create echo chambers for extremist and conspiratorial ideas. These ideas spread far and quickly, and are often reinforced by other actors in the echo chamber. Counter-extremists and outside information often cannot penetrate the network because it is either too diffuse and/or too dense for an outsider to break through. Thinking about the types of digital networks created

[5] Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7:3 (2015): 572–616. See, for example, Microsoft's Cyber Peace Institute (https://cyberpeaceinstitute.org/), or the testimony of Facebook's Mark Zuckerberg and Twitter's Jack Dorsey for the US Senate Judiciary Committee. Joseph Stepansky, "Facebook, Twitter grilled on election response by US Senators," *Al Jazeera*, November 17, 2020, https://www.aljazeera.com/economy/2020/11/17/facebook-twitter-heads-testify-before-us-senate-live.

by new technologies could be one way to understand what types of messages are most likely to resonate and lead individuals to commit acts of violence. Do denser, closed networks do a better job of indoctrinating potential recruits? Or do potential recruits get their feet wet by exploring the periphery of a more diffuse network, and slowly make their way toward a denser core? Similarly, what role do social network ties play in mobilizing individuals? Previous work in this area has looked at threshold models of mobilization and the importance of social ties in bringing people into movements.[6] It seems likely that digital technologies have, on the one hand, lowered the costs and barriers to forming ties with others. Simply clicking to join a Facebook group or watching a YouTube video can be a person's entryway into certain networks. On the other hand, the ease of access might make terror groups more suspicious of potential recruits, and actually raise the costs and resources needed to vet and fully mobilize individuals. Cronin mentions the case of "Alex," a young woman with whom an ISIS agent reportedly spent up to seven hours a day on Skype in order to slowly recruit her into the movement (188). This type of time and effort cuts against claims that digital technologies will lead to a sharp rise in the number of people joining terror groups. A research question that future work can consider is what types of ties matter most for recruiting individuals into groups.

One of the core strengths of the books is Cronin's engaging writing style and frequent use of examples. Each chapter begins with a brief illustrative example that then leads to broader theoretical points. Cronin makes it very easy for her readers to understand how each particular chapter fits into the overall argument, which makes this book an excellent resource for teaching, as well as a foundation for future scholarship. The dataset that she developed and shared as part of the book is an invaluable resource for future scholarship on both terrorism and technology.

[6] Sarah Elizabeth Parkinson, "Organizing Rebellion: Rethinking High-Risk Mobilization and Social Networks in War," *American Political Science Review* 107:3 (2013): 418–432, https://doi.org/10.1017/S0003055413000208; Mark Granovetter, "Threshold Models of Collective Behavior," *American Journal of Sociology* (1978): 1420–1443; Mark Granovetter, "The Strength of Weak Ties: A Network Theory Revisited," *Sociological Theory* 1:1 (1983): 201–233; Arie Perliger and Ami Pedahzur, "Social Network Analysis in the Study of Terrorism and Political Violence," *PS: Political Science & Politics* 44:1 (January 2011): 45–50, https://doi.org/10.1017/S1049096510001848; Steven T. Zech and Michael Gabbay, "Social Network Analysis in the Study of Terrorism and Insurgency: From Organization to Politics," *International Studies Review* 18:2 (2016): 214–243.

Response by Audrey Kurth Cronin, American University

A group of insightful scholars have read my latest book and engaged with its argument, and I am grateful. My sincere thanks to Professors Deborah Avant, Boyd P. Brown, and Jennifer Spindel for reading and reviewing *Power to the People*, and to Professor Michael Neagle for commissioning this roundtable.

My goal in *Power to the People* was to examine the innovation and diffusion of technologies that have influenced the trajectory of modern political violence over the past two centuries, and then draw implications for emerging technologies in the digital age. Most experts argue that terrorists and insurgents are conservative and prefer to use proven means, especially "guns and bombs." Would that continue to be the case, I wondered? The book resulted from ten years of data collection and a deep dive into a range of new digital technologies to see how they are changing nonstate actor conflict, especially terrorism. What I found is that terrorists are likely to expand their repertoire going forward–expanding their use of small unmanned aerial vehicles (UAVs), robotics, 3D-printing, facial recognition technology, and autonomous systems, for example–but also that stakeholders can draw upon the history of how lethal technologies spread to mitigate risks today.

A large slice of the picture of the historical and global evolution of political violence was missing from the scholarly literature. I could find no work that examined the innovation and diffusion of technology across disciplinary stovepipes (political science, history, sociology, economics) to understand broad trajectories. Most scholars have focused on ideologies, tactics, leadership, organizational structures, and individual groups' actions over the past fifty years. Some excellent work on technological innovation and diffusion has emerged from that dedicated scholarship,[24] shaped by the availability of robust data on terrorism from about 1970 onward[25] —but there was not much insight about what happened before 1970.

Yet historians agree that modern terrorism began in the nineteenth century, with the concept of propaganda of the deed (from the French, *propagande par le fait*). The Italian revolutionary Carlo Piscane originated it in 1857, and French/American and Russian intellectuals such as Marie Le Compte and Peter Kropotkin popularized it.[26] I wondered whether lessons emerging from the study of recent terrorists and twentieth-century technologies were anomalous when viewed over a longer period. In this book, I set about broadening the historical aperture in understanding technologies in political violence.

[24] Prominent works include Paul Wilkinson, ed., *Technology and Terrorism* (London: Frank Cass, 1993); Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics, and Global Trends* (London and New York: Routledge, 2007); Michael Horowitz, "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism." *International Organization* 64:1: 33-64, Manus I. Midlarsky, Martha Crenshaw, and Fumihiko Yoshida, "Why Violence Spreads: The Contagion of International Terrorism," *International Studies Quarterly* 24 (1980): 262-98; and Kim Cragin, Peter Chalk, Sara A. Daly, Brian A. Jackson, *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies* (Santa Monica: RAND Corporation, 2007). Also, Gary Ackerman of SUNY Albany has written a very interesting dissertation that draws on GTD data, "'More Bang for the Buck': Examining the Determinants of Terrorist Adoption of New Weapons Technologies," King's College dissertation, London, 2014. This is a brief sampling. Please see *Power to the People* for much more comprehensive footnotes and an extensive Bibliography.

[25] See particularly the Global Terrorism Database, https://www.start.umd.edu/data-tools/global-terrorism-database-gtd. For a wonderful analysis of that dataset, see Gary LaFree, Laura Dugan, and Erin Miller, *Putting Terrorism in Context: Lessons from the Global Terrorism Database* (London: Routledge, 2015). (The title is an echo of the book Martha Crenshaw edited in 1995, *Terrorism in Context* (University Park: Pennsylvania State University Press).

[26] Carlo Piscane wrote, "The propaganda of the idea is a chimera. Ideas result from deeds, not the latter from the former." George Woodcock, ed., *The Anarchist Reader* (Brighton, Sussex: Harvester Press, 1977) 43. See also David C. Rapoport, the Four Waves of Modern Terrorism," chapter 2 of *Attacking Terrorism: Elements of a Grand Strategy*, edited by Audrey Kurth Cronin and James M. Ludes (Washington, D.C.: Georgetown University Press, 2004), 46-73.

This brings me to the three perceptive roundtable reviews. I will begin with Brown's review of *Power to the People,* which captures the book's historical arguments well. He writes, "Cronin's analysis is ultimately about the law of unintended consequence," and I agree. His review of the chapters on dynamite and the Kalashnikov, which he describes as "the core of *Power to the People*," is astute.

Brown understands the relationship between the historical case studies on dynamite and the Kalashnikov, one the one hand, and the overarching argument "about the risk posed by our current, mostly open, age of technological innovation" on the other. The balance between narrative and factual detail is always a challenge, and I am pleased that Brown finds the discussion of dynamite "thorough and eye-opening without being overly technical." He reminds us, however, that novelty can be deceptive: for example, Northeastern University physics student Rezwan Ferdaus's 2011 attempt to use a remote-controlled aircraft to bomb the Pentagon means armed quadcopters are not that new, after all. He is right, and I take his point.

Finally, Brown seizes upon the book's economic argument about the changing connotation of property ownership in the digital age and its broader historical implications for capitalist societies. Purchasing something today does not mean it belongs to you. Private companies essentially 'lend' us their products, keeping them tethered so as to collect data while retaining company ownership of the software, the crucial element that makes them work. A new kind of human serfdom emerges, with consumers dependent on technology companies. That is what my book means by "the new feudalism," a concept that has been more extensively developed by scholars such as Joshua Fairfield and Shoshana Zuboff.[27]

In his closing arguments, Brown calls the book "an important study" that is valuable for "any historian, technology expert, or security professional who is interested in the dynamic nature of our new reality." I am grateful for his careful reading, insightful comments, and generous appraisal of my book.

In her review, Avant calls *Power to the People* "smart and important," urges us to contend with the double-edged nature of many emerging technologies, and sees a lot to learn from how open systems of innovation diffuse and can be used for violent purposes. But I will address Avant's more critical points regarding case selection, scope, and the role of states.

Regarding case selection, Avant asks why the book discusses dynamite and Kalashnikovs, rather than other innovations "say other types of small arms."[28] In fact the book does discuss many different types of small arms, including the first significant quantity multi-shot revolver (produced by Samuel Colt), the Remington and Winchester rifles (legendary on the US Western frontier), as well as the technological evolution and global spread of muskets, rifles, and a large range of sub-and light-machine guns (129-134). To be fair, however, it is true that *Power to the People* has two chapters on the Kalashnikov and no separate chapters for any of the other small arms it analyzes.

The reason is that no other firearm has had the impact on political violence that the Kalashnikov has had. Kalashnikovs kill a quarter of a million people every year,[29] and their spread exceeds by five or ten times the distribution of the next most

[27] Joshua Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (Cambridge: Cambridge University Press, 2017); and Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for A Human Future at the New Frontier of Power* (New York: Public Affairs 2019).

[28] The Small Arms Survey defines small arms as revolvers and self-loading pistols, rifles and carbines, assault rifles, sub-machine guns, and light machine guns (130-134). See Small Arms Survey at http://smallarmssurvey.org/weapons-and-markets/definitions.html.

[29] Larry Kahaner, "Weapon of Mass Destruction," *Washington Post*, 26 November 2006; see also Kahaner, *AK-47: The Weapon That Changed the World* (Hoboken: John Wiley, 2007).

common family of rifles, the American-made M-16.[30] Also, no other firearm has the Kalashnikov's symbolic resonance: the AK-47 (or its facsimile) appears on the flags of Mozambique and Hezbollah, and on the coats of arms of Zimbabwe, Burkina Faso (1984-1997), and East Timor.

Power to the People is not designed to be a randomized examination of all lethal technologies. It studies why and how two standout technologies had the outsized impact on global political violence that they had, even as other, better technologies did not. It takes pains to address why a range of firearms and explosives did *not* diffuse, also analyzing why explosives such as ballistite, guncotton and gelignite failed to catch on in the way that dynamite did (123-124). Digging as deeply into other explosives and firearms would not tell us much about how technology diffuses to nonstate actors and how political violence spreads, which is what the book is about.

Regarding the scope of analysis, the book is not about governing the Internet. It is about emerging digital technologies, not all of which are web-connected. Some use cellular networks, satellite links or even radio waves—as quadcopters do. In this regard, I was delighted that Avant quoted my colleague Professor Laura DeNardis's 2014 work on the global governance of the Internet.[31] I am familiar with the Global Network Initiative, which is dedicated to protecting free expression.[32] But a study of international Internet governance would be a different book. Fortunately, DeNardis has already written it.[33]

The list of international organizations and private nonprofit initiatives dealing with robotics and artificial intelligence, for example, is vast. These include the UN Convention on Certain Autonomous Weapons and Lethal Autonomous Weapons Systems;[34] the United National International Regional Crime and Justice Research Institute (UNICRI) Centre for Artificial Intelligence and Robotics in The Hague;[35] The Campaign to Stop Killer Robots;[36] the World Economic Forum,[37] and The Future of Life Institute.[38] *Power to the People* devotes a chapter to the risks of autonomous systems and artificial intelligence, concluding that, "The answer to these security challenges is not necessarily more traditional security" (267).

Finally, Avant argues that the book "ignores the fact that technology also changes and enables malevolent *state* action." The introduction explains that the book's primary question is "How and why do non-state actors innovate differently from state actors?" (4) The book criticizes the behavior of authoritarian actors such as China and points to the serious problem of

[30] C.J. Chivers, *The Gun* (New York: Simon & Schuster, 2010). Chivers won the Pulitzer Prize for this book.

[31] Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

[32] Global Network Initiative, https://globalnetworkinitiative.org/.

[33] Readers may also be interested in DeNardis's latest book, *The Internet in Everything: Freedom and Security in a World with No off Switch* (New Haven: Yale University Press, 2020).

[34] United Nations, Convention on Certain Conventional Weapons—Meeting of Experts, https://meetings.unoda.org/meeting/ccw-pv-mx-2020/.

[35] United National International Regional Crime and Justice Research Institute (UNICRI), Centre for Artificial Intelligence and Robotics, The Hague, The Netherlands, http://unicri.it/in_focus/on/UNICRI_Centre_Artificial_Robotics.

[36] The Campaign to Stop Killer Robots, https://www.stopkillerrobots.org/.

[37] The World Economic Forum, *Global Technology Governance Report 2021*, https://www.weforum.org/reports/global-technology-governance-report-2021.

[38] The Future of Life Institute, https://futureoflife.org/.

autocratic abuse of digital technologies. (6-7, 222, 262-63). It references a vast amount of literature (including my writing) on the ethical, legal, and strategic problems of state use of high-altitude, armed UAVs (209-217, footnotes 30-48). But assessing state action is not its main purpose.

In suggesting countermeasures to nonstate actor technological innovation, *Power to the People* advocates shoring up democracies, but it does not argue that states are the only governors of technology–in Avant's words, "the purveyors of order and protection against malevolence." It explains horrible abuses of state power such as the Pennsylvania National Guard's use of a Gatlin gun against strikers during the 1892 Homestead Steel Strike (131), widespread U.S. government repression of immigrants in the 1919 Palmer Raids (92-93), the Soviet government's brutal crushing of the Russian anarchists in the 1920s (91), and the Soviet Army's slaughtering of insurgents in the 1956 Hungarian Revolution (144-46). The book is not a one-sided argument about benevolent state power.

Spindel's review captures the political science themes of *Power to the People*, sees the broader repercussions of the book regarding power asymmetries and war, and throws out a series of stimulating questions about its implications. I will not rehearse her insightful commentary on the book but instead address a few of her questions. Many point either to additional research I have been doing or to related studies I hope others will do. I find them exciting.

For example, Spindel asks, "[W]hy do some messages inspire global movements, while others remain stuck in obscurity?" In the current historical context, *Power to the People*'s answer is that nefarious human beings and authoritarian state actors choose to amplify some messages and not others via the innovative use of new digital technologies. Often it is not the content of the messages that matters, but their potential to sow chaos. Understanding the complex motivations that lie *behind* promoting dangerous ideologies is the future imperative.

Another stimulating question is, "Are we living in a moment in time where violent non-state actors might have the power to change how people think about what it means to engage in 'war' or violence?" The answer to that question is yes. One need only consider the popularity of guns and tactical gear among violent domestic extremists in Germany, Norway, and especially the United States. Groups like Patriot Prayer, Proud Boys, Kenosha Guard and especially the Boogaloo movement draw people to them by reframing what it means to be a soldier at war within the United States. Indeed, the Boogaloo movement aims to start a second civil war in the United States.

All of these U.S. groups also train, share memes, and virtually connect with other right-wing groups who actually are at war, for example in Ukraine. With growing militia movements in states like Michigan, Pennsylvania, Wisconsin, and Oregon, it is clear that violent nonstate actors have already altered how a large number of people think about engaging in war. Spindel writes that "Cronin opens the door for future work to analyze when and how has the dominant conceptualization of war been changed by the technological innovations of non-state groups." I would be delighted if someone took up that topic and went beyond what I could fit into my book.

Of course, few reviews are all positive. Spindel argues that "Cronin's real insights about the spread and diffusion of technologies, and how that is related to violence, sometimes seem to get distracted by a focus on jihadist terrorism, and sometimes leave bigger questions unanswered." I accept that criticism. The book was written with the backdrop of the war in Syria, the rise of the Islamic State of Iraq and Syria (ISIS), and jihadist attacks in Europe. Until 2019, ISIS was the most innovative terrorist group in its use of accessible digital technologies, mainly social media, and armed quadcopters. Early indicators came from that realm, so there are many jihadist examples cited in this book.

The book is not organized around group ideologies (jihadist, right-wing, Neo-Nazi, etc.) but around technologies. Yet *Power to the People* does describe domestic violent extremists' actions in the United States and Europe. It analyzes White Supremacist, racist, anti-Muslim, and anti-Semitic targeting (190-2) and right-wing or extreme libertarian file sharing of 3-D printed firearms via encrypted platforms (226-229). It explains the acceleration of domestic violent extremists by state actors (especially Russia) through the use of bots, troll farms, fake news, and viral memes (193-5), as well as the broader

implications of those activities for small group mobilization, reach, and systems integration. A key theme throughout the book is how digital technologies are today providing "new triggers for old passions" (175-77).

Power to the People is about nonstate actors and their use of violence "from below." Today's democratic governments and their populations lag in understanding the political impacts of accessible lethal digital technologies. Americans created many of them, but they are naïve about how and why we must channel them for use in the public interest. There are serious risks in the United States' present laissez-faire approach. The answer is to seek a middle way—i.e., neither to swing wildly toward repressive state power, as in authoritarian states, nor to shrug at the need to protect people from nefarious individuals and small groups, as the United States does now. The January 6, 2021 Capitol Hill insurrection illustrates one consequence of the technological risks explained in *Power to the People*. If the U.S. remains on its current trajectory, there will be more such events.