H-Diplo | ISSF Roundtable XI-13

issforum.org

Robert Mandel. ***Global Data Shock: Strategic Ambiguity, Deception, and Surprise in an Age of Information Overload.*** Stanford: Stanford University Press, 2019. ISBN: 9781503608252 (cloth); 9781503608962 (paper).

13 March 2020 | https://issforum.org/to/ir11-13
Editors: Rebecca Slayton and Diane Labrosse | Production Editor: George Fujii

Contents

Introduction by Jon R. Lindsay, University of Toronto

In an age of information overload, H-Diplo/ISSF roundtables help you decide which books to add to your reading list and which to leave aside. Robert Mandel's *Global Data Shock* is itself a book about information overload, and it does provide readers with a lot of information. For a book about strategic ambiguity, deception, and surprise, however, it may or may not be surprising that the experts in intelligence affairs gathered together here offer ambivalent reviews. All praise the relevance of Mandel's topic, as well as his skepticism for technocratic solutions to the problem, but they also highlight numerous conceptual and empirical shortfalls. Much as policymakers continue to struggle to make sense of a flood of data in global politics, it seems we still lack clarity on these important matters.

Mandel is a prolific author with a knack for showcasing the popular security problems of the day. His most recent books have dealt with non-state actors, state coercion, cyberdeterrence, human security, and now strategic deception as well. Motivated by the Russian campaign to influence the 2016 U.S. presidential election and anticipating the dark currents already in motion for 2020, the book is undeniably timely. With the explosion of interest in artificial intelligence in the intelligence community and beyond, moreover, it is undeniably relevant. Yet a lengthier publication timeline may have provided the opportunity to identify and correct some of the problems that come to light in this roundtable.

Austin Carson calls the book "refreshing and provocative," describing strengths such as "updating and tailoring" some classic insights about misperception "for an era of 'big data' optimism" as well as highlighting the potential for deception in technologies that are widely assumed, ironically enough, to improve knowledge. As Carson writes, "This is valuable tonic for the ills that accompany a simplistic, presentist appraisal of the all-seeing 'information age'." Kathleen Vogel also praises the general enterprise of the book, calling it "a useful contribution to creating a larger global critique on the use of Big Data." She writes that it "provides an important perspective" by "exploring the more complicated picture surrounding the promises of Big Data." For intelligence practitioners, as Vogel notes, this "will require new thinking and analytic methods to make sense of this new convoluted data environment." Amy Zegart agrees that the book is "a worthy endeavor." She describes it "an ambitious book that asks two important and timely questions," namely whether information overload and strategic deception are new and whether they matter in world affairs.

Yet Zegart also finds that "*Global Data Shock* promises more than it delivers." Carson has similar concerns: "important strengths are accompanied by a set of significant weaknesses." The book starts with a brief introduction, including a list of the book's ostensibly novel contributions that Carson and Zegart both describe as "immodest." Both cite previous work and precedents that Mandel overlooks. Carson points out that "scholars of intelligence studies, for example, have argued for decades that major intelligence failures are often the result of too much, rather than too few, data points." Carson further asks, "What, if anything, is new about the way information and policy failures are linked today? If this is simply a story about psychological and organizational biases, the book's contribution is significantly weakened." Zegart's review is even more to the point: "the gist of his argument can be summed up in one sentence: More information is not always better….None of this is news."

The first two chapters present the conceptual argument that the modern digital environment, considering the psychological biases of humans who must cope with it, tends to enhance the potential for strategic manipulation. Carson finds that the "analysis is stretched precariously thin." He raises concerns about "a lack of clarity about the relative causal weight of 'information overload.'" Zegart agrees that "the role of the information environment is not well defined or operationalized." Both also lament, as Zegart writes, that "alternative explanations are not seriously considered." Zegart suggests that organizational dysfunction or manipulation as much as information overload or strategic deception might also explain many analytical failures. For instance, President Donald "Trump's inconsistent foreign policy could also be explained by bureaucratic weakness, not strategic strength." Suggesting another alternative, Carson observes "that quality of information and volume of information are not equivalent. Perhaps the problem is a shock of bad data."

The next two chapters present and analyze ten brief case studies, which as Mandel argues in his response to the roundtable, "are designed to be illustrative, and thus cannot serve a basis for rigorously proving or disproving hypotheses." Even so,

Zegart echoes Carson's complaint about the thinness of analysis: "Evidence is often thin. And some of the key lessons learned appear to be the wrong ones." Carson argues that there are too many cases for any one of them to be convincing, yet too few to make the historical comparisons needed to gauge whether technology really matters. He thus highlights a "recurring concern [with] the book's presentist view of the politics of information." Indeed, all of Mandel's cases are from the twenty-first century, with the sole exception being Iraq's invasion of Kuwait in 1990. Each of the reviewers took issue with Mandel's interpretation of particular cases. For example, on the case of Iraqi weapons of mass destruction in 2002-03, Vogel points out that "adversaries do not need to have or use Big Data—they can create deception through Small Data, low tech, and low cost means to advance their security objectives." On the same case Carson asks, "How was overload the problem when their central challenge was gaining access to sites within Iraq that could enable a verification judgment?"

The final substantive chapter on "Managing Global Data Shock" is perhaps the most valuable in the book in terms of practical implications. As Vogel points out, "Mandel argues that more attention and resources need to be invested in providing critical-thinking skills to intelligence analysts and policymakers." Drawing on Gregory Treverton's famous distinction between intelligence secrets and mysteries, Vogel observes that the intelligence problems governments "have and will face are mysteries, and merely having more data will not be helpful in and of itself."[1] This has important implications for emerging artificial intelligence initiatives, she notes, because technological initiatives must be complemented by "workforce training that teaches analysts to have a critical perspective on these technologies."

Vogel closes by referencing Sheila Jasanoff's argument "that every new technology comes with many sources of ambiguity, indeterminacy, and complexity."[2] The same can be said for Mandel's book itself. Sadly, ambiguity does not clarify ambiguity nor does complexity simplify complexity. While *Global Data Shock* has areas of strength, the contributors argue that digital deception has yet to receive its definitive treatment.[3]

Participants:

Robert Mandel is Chair and Professor of International Affairs at Lewis & Clark College in Portland, Oregon. He has published fifteen books and over fifty articles and book chapters on global security and conflict issues. He has testified before the United States Congress and worked for multiple government intelligence agencies.

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

Austin Carson is Assistant Professor in the Department of Political Science at the University of Chicago. He is the author of two books on secrecy in international politics, *Secret Wars: Covert Conflict in International Politics* (Princeton University Press 2018) and *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation* (Cambridge University Press, forthcoming), with Allison Carnegie.

[1] Quote from Vogel, referencing Gregory F. Treverton, "Risks and Riddles: The Soviet Union was a puzzle. Al Qaeda is a mystery. Why we need to know the difference," *Smithsonian Magazine* (June 2007), https://www.smithsonianmag.com/history/risks-and-riddles-154744750/.

[2] Quote from Vogel, referencing Sheila Jasanoff, "Technologies of Humility," *Nature* 450 (1 November 2007): 33.

[3] I have expressed my views on the book elsewhere. See Jon R. Lindsay, "Review of Global Data Shock: Strategic Ambiguity, Deception, and Surprise in an Age of Information Overload," *Perspectives on Politics* 18:1 (March 2020): 336-337.

Kathleen M. Vogel is an associate professor in the School of Public Policy, University of Maryland at College Park. During 2018-2019, Vogel was a Rutherford Fellow at the Alan Turing Institute, London, UK. Her research focuses on studying the social and technical dimensions of bioweapons and emerging life science threats, the production of knowledge in intelligence assessments, and trends in human trafficking. Vogel is author of *Phantom Menace or Looming Danger?: A New Framework for Assessing Bioweapons Threats* (Baltimore: The Johns Hopkins University Press, 2013). She is also co-editor of *Facilitating Interdisciplinary Collaboration among the Intelligence Community, Academy, and Industry* (Newcastle upon Tyne, UK: Cambridge Scholars Publishing, forthcoming), a book about the Laboratory for Analytic Sciences, a Big Data laboratory funded by the U.S. National Security Agency.

Amy Zegart is the Davies Family Senior Fellow at the Hoover Institution, senior fellow at the Freeman Spogli Institute, and Professor of Political Science, by courtesy, at Stanford University.

Review by Austin Carson, University of Chicago

Robert Mandel's *Global Data Shock* is a refreshing and provocative analysis of the relationship between information and the quality of political decisions and policy solutions. *Global Data Shock* makes the case that too much information is often dangerous. Mandel points to new phenomena like big data and the proliferation of media sources, arguing that an avalanche of data can overwhelm and produce ambiguity, breed deception, and invite tactical surprise. In a set of wide-ranging case studies, Mandel makes the case that everything from Brexit to the Fukushima meltdown to 9/11 have been enabled by an overload of information.

Global Data Shock is a useful intervention in work on the political implications of information and technology. It joins with others in challenging a common view that transparency and richer information environments produce better political outcomes. Mandel is not the first to take issue with the assumption that "more information is better." Scholars of intelligence studies, for example, have argued for decades that major intelligence failures are often the result of too much, rather than too few, data points.[1] International Relations (IR) scholars, myself included, are increasingly assessing the negative consequences of reducing barriers to information.[2] Mandel's contribution beyond this work is updating and tailoring these claims for an era of "big data" optimism and finding connections across a diverse range of cases and domains.

A second strength of the book is its presentation of some new ideas about how deception and surprise persist in a world of ubiquitous information. The proliferation of data and the ever-growing nature of computing power have produced a revolution in the visibility of social behavior and governmental activity. This has led many to wonder if traditional modes of state secrecy and deception remain a realistic part of political life.[3] After all, the rise of crowdsourcing, citizen journalism, and commercial satellite imagery has rendered traditionally opaque spaces visible and undermined many older approaches to secrecy. But Mandel flips the conclusion on its head, drawing inspiration from psychology and organization theory to point out how too much information—and our tendency to fail to process and make sense of an ocean of data—can create new opportunities for deception and surprise. This is valuable tonic for the ills that accompany a simplistic, presentist appraisal of the all-seeing 'information age.'

Yet these important strengths are accompanied by a set of significant weaknesses in *Global Data Shock*. The book's writing and its approach to empirical evidence fall short in several ways. Too often, the analysis is stretched precariously thin in the sprint to cover so many issues and to connect a half-dozen concepts so broadly. One wishes that Mandel had cleaved his claims and his case studies in half, providing him and the reader more time and space to carefully engage the more provocative and interesting claims.

[1] See, for example, Richard K. Betts, "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly* 95:4 (1981): 551-572; Charles F. Parker and Eric K. Stern, "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise," *Foreign Policy Analysis* 1:3 (2005): 301-331.

[2] See, for example, Bernard I. Finel, and Kristin M. Lord, "The Surprising Logic of Transparency," *International Studies Quarterly* 43:2 (June 1999): 315-339; David Stasavage, "Open-Door or Closed-Door? Transparency in Domestic and International Bargaining," *International Organization* 58:4 (2004): 667-703; Kristin M. Lord, *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*. (New York: SUNY Press, 2006); Shuhei Kurizaki, "Efficient Secrecy: Public Versus Private Threats in Crisis Diplomacy," *American Political Science Review* 101:3 (2007): 543-558; Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War." *International Organization* 70:1 (2016): 103-131; Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton: Princeton University Press, 2018).

[3] See, for example, Ann M. Florini, "The End of Secrecy," in Bernard I. Finel and Kristin M. Lord, eds., *Power and Conflict in the Age of Transparency*, (New York: Palgrave, 2002); "No More Secrets: National Security Strategies for a Transparent World." American Bar Association Standing Committee on Law and National Security Workshop Report, March 2011.

One recurring and significant problem in *Global Data Shock* is a lack of clarity about the relative causal weight of "information overload"—the central conceit of the book—compared to other factors. Mandel's thesis depends on answering this question: How important was the volume of information in producing poor outcomes in everything from nuclear reactor meltdowns to terror attacks? Yet answering it convincingly is no small challenge. Pick any personal or organizational failure and one can always point to a pile of conflicting information that was available beforehand. When do we conclude that the available data was excessive, and how do we trace the importance of psychological and organizational biases from "overload" versus other likely causes of failure?

It is surprising that a number of the case studies in *Global Data Shock* suggest that the opposite problem—too little information—may be more important than overload. In the crucial months before the invasion of Iraq, for example, are we really to believe that United Nations weapons inspectors had too much information? How was overload the problem when their central challenge was gaining access to sites within Iraq that could enable a verification judgment? Mandel rightly points out that Iraqi President Saddam Hussein carefully deceived outsiders for over a decade before the 2003 invasion. He also rightly points to conflicting accounts given by Saddam, Iraqi defectors, and the resulting confusion in intelligence assessments and media accounts. But it stretches plausibility to argue that the mistaken certainty about weapons of mass destruction (WMD) was simply a biased reaction to the overwhelming effects of information overload. Re-running history with *more* information—i.e. foreign inspectors with an all-access pass to Iraqi WMD sites—would have exposed the false assumptions driving pre-invasion intelligence analysis.

This basic criticism can be levied about many of the other case studies in *Global Data Shock,* including the 9/11 attacks. This is a reminder that *quality* of information and *volume* of information are not equivalent. Perhaps the problem is a shock of bad data.[4] Mandel tends to see an ocean of conflicting information preceding policy disasters of various kinds. This is fair. But there is another interpretation: when we lack precise, high-quality information, the only straws to grasp are low-credibility sources like social media and dubious defector accounts. The root cause is poor information; the proximal but ultimately ephemeral cause is the ocean of other information we reach for in its absence.

Another recurring concern is the book's presentist view of the politics of information. The subtitle posits that we have entered an "age of information overload." Does Mandel make a persuasive case that the same scenarios unfolding *before* the "global data shock" would end any differently? I worry he does not. The Fukushima case study illustrates this most clearly. Mandel looks for and finds deception in the Japanese government's inaccurate public statements during the crisis. Even if we assume the worst about such statements, Japan's reaction was identical to other government responses to nuclear disasters over the past half century. The Soviet reaction to Chernobyl predated the "age of information overload" and was rife with deception. Panic and confusion was the dominant reaction to the Three Mile Island partial meltdown in the United States. None of these took place in an age of information overload.

Other historical comparisons underscore this point. A failure to separate useful data from a firehose of information has long been the culprit for the failure to prevent the attacks at Pearl Harbor in the 1940s, as Mandel himself notes (130). How does this failure differ from the failure to prevent the 9/11 attacks?

This begs a broad question about the book's conclusion: What, if anything, is new about the way information and policy failures are linked today? If this is simply a story about psychological and organizational biases, the book's contribution is significantly weakened. Moreover, historical comparisons beg for thinking about ways digital-era technologies make deception and surprise harder. A Chernobyl-like lockdown after a nuclear reactor meltdown would be impossible today. Yet

[4] A related point is that volume of information is less important than how different governmental actors interpret that information. See Keren Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations*. (Princeton: Princeton University Press, 2014).

the book's central premise is that a "global information explosion" (6) is a product of new transportation and communication technologies with new implications for how surprise, ambiguity, and deception work.

Much of the ambiguity (pun intended) about causal weight and historical novelty is the product of Mandel's attempt to analyze a diverse set of ten case studies across a startlingly broad range technical domains. In each case study, Mandel applies a set of common questions about information overload, its immediate problems (i.e. deception, ambiguity, and surprise), and the ultimate policy result. This approach is admirably clear. The author's broad coverage and consistent method of asking similar questions is admirable.

Yet this approach has serious costs. As in many things, less is probably more. Readers may find some empirical claims too rushed and unconvincing. For example, Mandel analyzes Donald Trump's "foreign security policy style" (59) and makes the case that Trump's unpredictability is an intentional and strategic reaction to the era of information overload. We do not get a careful refutation of the obvious alternative explanation for such vacillations: incompetence, impulsiveness, staff turnover, and the choice to bypass the foreign policy bureaucracy. Mandel only devotes three paragraphs to the section explaining information overload's role in a presidency that has attracted books about its foreign policy.[5] Similarly abbreviated treatment is given to other complex and contested events, such as the factors producing Brexit and the 2007 Syrian strike on the al-Kibar nuclear reactor. Such discussions are not satisfactory.

Finally, Mandel's writing style sometimes detracts from possible substantive contributions. The book begins by a rather immodest list of no fewer than five ways in which *Global Data Shock* is the "first book" (3) to address its topics, including several which clearly feature previous scholarship. Mandel's descriptions are detailed but also distractingly overstuffed with adjectives. The book's conclusions do not just differ from existing views of international restraint, but with "alleged enlightened global restraint" (4). A common misunderstanding about tactics of manipulation is a "prevalent deficient manipulation response" (173). The main obstacles to accurate perception are described as "core interconnected information interpretation barriers" (18).

Despite these problems, the book's central claims do raise important questions for future research. Two stick out as especially important. First is credibility. In an era of democratized communication and information overload, *authority* becomes an even more precious resource. If access to information is cheap, states and others must vie for attention and persuasion. Mandel notes the damage done to American credibility by the intelligence failure regarding WMD in Iraq (83). Yet we know precious little about how states build credibility regarding their intelligence or other public claims, how they maintain it, and how they regain it after a crisis. If Mandel is right that ambiguity, deception, and surprise are regular features of our contemporary security landscape, then careful thinking about how states can counteract dubious disinformation campaigns is important.

A second area for further development, drawing from the ideas in *Global Data Shock,* is analysis of reactions to deception and surprise. Mandel discusses cases which feature a range of reactions to deception efforts. When are disinformation campaigns met with resolute repudiation, and when do they produce a fractured or paralyzed response? For example, Mandel notes that the international community "reacted quickly and negatively" to Russia's deceptive annexation of Crimea (90). In other cases, such as Syria's bombing of the al-Kibar nuclear plant, acts of surprise and deception are met with a "simmering silence" (149). This begs for systematic research that identifies the conditions under which attempts to take advantage of the downsides of information overload are refuted or acquiesced to. If the volume of information is a genie which cannot be put back in the bottle, then insight into how credibility can be rationed and cohesive political responses encouraged will only grow in importance.

[5] See, for example, Robert Jervis et al., eds. *Chaos in the Liberal Order: The Trump Presidency and International Politics in the Twenty-First Century* (New York: Columbia University Press, 2018).

Review by Kathleen M. Vogel, University of Maryland

Robert Mandel's new book provides an important perspective on the question of how states will cope with the onslaught of Big Data and its effects on intelligence assessments and national security policymaking now and in the future. Although there have been various articles that have drawn attention to the increasing role of Big Data in intelligence, *Global Data Shock* is the first to systematically examine the possibilities and pitfalls of this relationship. Mandel defines global data shock as the "disconnect between common information and communication premises and existing realities" that impedes "both public officials' and private citizens' ability to interpret, respond to, and ultimately shape the world around them" (1-2). Mandel's book provides a useful contribution to security studies and information studies by exploring the more complicated picture surrounding the promises of Big Data; and how the availability of Big Data for intelligence can actually create new challenges for analysis and policymaking.

Mandel describes how there are two polarized camps in discussions related to Big Data and national security: (1) the technological optimists, who believe that Big Data and Big Data analytics will 'bless us' by providing more accurate and timely understandings of adversaries, their intentions, and actions; and (2) the technological pessimists, who see Big Data as 'a curse,' emphasizing how errors and burdens can be introduced into the process of collecting and working with large and diverse data sets (11-15). Mandel positions himself in the middle ground to these two camps. He acknowledges benefits of using and processing Big Data, but cautions against putting our total faith in it and related technologies. He argues that there are a host of human, organizational, and technical challenges in the acquisition, management, and processing of large amounts of information that will introduce new challenges into the use of Big Data for national security policymaking—and additional challenges for publics to understand the strategic implications of these issues. Information overload brings new opportunities for ambiguity, deception, and surprise by adversaries, and also creates new possibilities for both benign and malicious fabrication of data—this makes "data interpretation much harder today and manipulation much easier than before" (11). With this more complicated view of information, Mandel underscores the problem of just 'connecting the dots' with Big Data and artificial intelligence tools. In the future, there are going to a lot more 'dots,' with many of them potentially distorted or fabricated; this will require new thinking and analytic methods to make sense of this new convoluted data environment.

Using a series of ten case studies of issues of national security importance across different country contexts within the twenty-first century, Mandel highlights the range of problems that are possible with information overload. I will focus my comments on one of his case studies: U.S. intelligence failures on Iraq's weapons of mass destruction (WMD) leading up to the 2003 war. In this case, as Mandel writes, the problem was not in collecting more data. There was already a host of data available through a variety of U.S. government, non-government, academic, and United Nations (UN) sources---including the fact that for over ten years before the 2003 war, Iraq was a U.S. national intelligence priority for collection. Consistent with Mandel, the problems that I and others have described,[1] is that intelligence analysts during this period were focused exclusively on pieces of narrow, technical information and also on fabricated intelligence to inform their analysis. Intelligence analysts 'kept their eye on the prize,' (i.e., Iraq), but the problem was that they failed to consider and integrate a broad variety of social, political, economic information along with technical data and other intelligence reports. Analysts disregarded anomalies that did not fit their existing frame of Iraq having a growing and advanced WMD program. This more complex set of information was available from 1991-2003; the problem is that it was ignored. Thus, analytic frames matter—it is not just merely about having more data. The frame that analysts use can shape what information gets accepted

[1] See Kathleen M. Vogel, *Phantom Menace or Looming Danger?: A New Framework for Assessing Bioweapons Threats* (Baltimore: The Johns Hopkins University Press, 2013); Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *The Journal of Strategic Studies* 29:1 (February 2006): 3-52; Richard Kerr, Thomas Wolfe, Rebecca Donegan, and Aris Pappas, "Issues for the U.S. Intelligence Community: Collection and Analysis on Iraq," *Studies in Intelligence* 49:3 (2005): 47-54, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Collection_Analysis_Iraq_5.htm; Charles Duelfer, *Comprehensive Report of the Special Advisor to the DCI on Iraq's WMD* (30 September 2004), https://www.cia.gov/library/reports/general-reports-1/iraq_wmd_2004/.

and validated, as well as information that gets marginalized and disregarded. As a result, intelligence analysts could not see how the combination of data about the U.S. bombing of Iraq, intrusive UN inspections and disarmament efforts, UN sanctions, and the massively corrupt Iraq regime had created a context whereby Iraqi President Saddam Hussein simply could not afford to pursue a WMD program after the First Gulf War.

The Iraq case also shows how a lot of bad and flawed intelligence was able to move around, and was stored and stove-piped within various classified information technology systems, without a way for intelligence analysts to be able to perceive these errors. Other analysts then used this flawed information for subsequent intelligence assessments. This points to the Big Data problem as not just one of data, but also of the various information systems and organizational dysfunctions that can create stovepipes and barriers, which can also introduce new errors into intelligence analysis. The Iraq case also shows that smaller, weaker states can use strategic ambiguity and deception with information against a more powerful enemy. As Mandel writes, "The Iraqi government clearly and consistently initiated strategic ambiguity and deception to hide the true scope of its overall weapons capabilities and related intensions" (75). To purposefully confuse the U.S. and other regional allies, Saddam Hussein kept his intentions and actions surrounding WMDs ambiguous. Mandel concludes that "ironically, Iraq's most successful deception was not about hiding its weapons of mass destruction but rather about hiding its lack of weapons of mass destruction" (81). This example shows how adversaries do not need to have or use Big Data—they can create deception through Small Data, low tech, and low cost means to advance their security objectives.

In reflecting on these information collection and analysis challenges, I was reminded of Gregory Treverton's discussion of mysteries and puzzles in intelligence:

There's a reason millions of people try to solve crossword puzzles each day…Even when you can't find the right answer, you know it exists. Puzzles can be solved; they have answers. But a mystery offers no such comfort. It poses a question that has no definitive answer because the answer is contingent; it depends on a future interaction of many factors, known and unknown. A mystery cannot be answered; it can only be framed, by identifying the critical factors and applying some sense of how they have interacted in the past and might interact in the future…Puzzles may be more satisfying, but the world increasingly offers us mysteries.[2]

What Mandel argues in his book is that more of the national security challenges that the U.S. and other countries have and will face are mysteries, and merely having more data will not be helpful in and of itself. Instead, Mandel argues that more attention and resources need to be invested in providing critical-thinking skills to intelligence analysts and policymakers to help them understand Big Data limitations and cautions, as well as different mental models for understanding intelligence mysteries. Mandel argues that we also need to provide analysts with a larger set of skills training that will help them evaluate and sort through the onslaught of problematic sets of Big Data, and how to integrate Big Data with Small Data. Mandel argues that "given rapidly changing conflicting data, intelligence analysts need to reject the notion that obtaining extra information guarantees a true and up-to-date threat picture of advisory intentions or actions, instead accepting more inconclusive, nuanced tentative, and qualified judgments" (200). In 2019, the Office of Director of National Intelligence released its *AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*, which is focused on increasing investment and deployment of artificial intelligence systems (AI) into intelligence. In reading through this strategy, very little text or time is focused on the human-centered challenges of working with, and trusting, AI systems. *Global Data Shock* would caution us not only to train analysts to learn Big Data/AI techniques, but also to create workforce training that teaches analysts to have a critical perspective on these technologies, and to keep humans in the loop in future human-machine teaming as part and parcel of the development and deployment of new AI systems.

[2] Gregory F. Treverton, "Risks and Riddles: The Soviet Union was a puzzle. Al Qaeda is a mystery. Why we need to know the difference," *Smithsonian Magazine* (June 2007), https://www.smithsonianmag.com/history/risks-and-riddles-154744750/.

After reading Mandel's book, I was reminded of Sheila Jasanoff's argument for the need humility with the uncertainties surrounding emerging technologies.[3] Jasanoff argues that every new technology comes with many sources of ambiguity, indeterminacy, and complexity, raising risks that require multi-stakeholder engagement. Jasanoff argues we need to allow time to consider a wide range of social perspectives about the technology and that this will require different kinds of engagement between experts, decision-makers, and the public. *Global Data Shock* highlights that we need to be aware of the dangers of naively trusting Big Data and AI systems and the need for deliberative engagement with intelligence practitioners and policymakers to create and manage information systems that can handle and anticipate potential risks and dangers with these technologies. We need more research that takes a critical perspective of how Big Data and AI systems are increasingly becoming ingrained in a variety of defense and security domains, as well as and the social, ethical, and policy implications that these will inherently bring. This book is a useful contribution to creating a larger global critique on the use of Big Data and related tools for national and international security.

[3] Sheila Jasanoff, "Technologies of Humility," *Nature* 450 (1 November 2007): 33.

Review by Amy Zegart, Freeman Spogli Institute of International Studies and the Hoover Institution, Stanford University

Robert Mandel's *Global Data Shock* is an ambitious book that asks two important and timely questions: (1) Is information overload in the Internet era really new? and, (2) if so, how does it affect international security—specifically the employment of strategic ambiguity, deception, and surprise by state and non-state actors?

Surveying a wide swath of literature from international relations to cognitive psychology to intelligence analysis, the author seeks to add greater nuance to the debate about whether new technologies bring unmitigated peril or unconstrained promise. Given how much terms like 'big data analytics' and 'AI' are thrown around these days, and how much nuance and historical perspective are both in short supply, it is a worthy endeavor.

Chapter 2, which examines how strategic ambiguity, deception, and surprise work, is especially strong. Mandel finds that growing information overload presents information consumers with many potential sources that make it far more difficult to distinguish between truth and falsehood, credible sources and untrustworthy ones. Ambiguity, he notes, is often aggravated by too much data. This background of strategic ambiguity, in turn, can facilitate the use of strategic deception—which Mandel defines as the manipulation of information and its interpretation in directions desired by state and non-state actors. Strategic deception, in turn, can lead to strategic surprise—sudden shocks that are unexpected by policymakers and citizens alike.

Mandel rather immodestly notes that *Global Data Shock* offers path-breaking insights about technology, information, theory, and policy under the heading, "Provocative and Unique Qualities" of the book (3). However, the gist of his argument can be summed up in one sentence: More information is not always better. The information explosion is making it harder to assess credibility and find signals amidst the noise, adapt bureaucratic organizations to new demands, and overcome the cognitive biases that affect even the smartest analysts. None of this is news.

Mandel offers ten short case studies that include President Donald Trump's foreign policy style in 2017, the Brexit referendum to leave the European Union, the non-discovery of Iraqi weapons of mass destruction, Russia's 2014 annexation of Crimea and 2008 invasion of Georgia, the 2011 Fukushima nuclear disaster, Israel's 2007 attack on Syria's nuclear plant, the September 11, 2001 terrorist attacks on the United States, the 2005 Andijan massacre in Uzbekistan, and Iraq's invasion of Kuwait in 1990. Here, too, the results are decidedly mixed. While the research design is admirable (case studies include both successes and failures at strategic ambiguity, deception and surprise across a broad set of geographies and circumstances), the role of the information environment is not well defined or operationalized. Alternative explanations are not seriously considered. Evidence is often thin. And some of the key lessons learned appear to be the wrong ones.

Mandel's treatment of the Trump foreign policy case seems more provocative than definitive. He asserts that Trump cleverly and deliberately pursued a strategic doctrine of unpredictability. But this neglects the alternative explanation that Trump's inconsistent foreign policy could also be explained by bureaucratic weakness, not strategic strength. As many observers have noted, the Trump Administration experienced higher White House staff turnover[1] in its first year than those of any of the previous five presidents—by a wide margin—as well as an unprecedented burn rate in its top foreign policy positions. In just 30 months, the Trump administration went through two secretaries of state, three national security advisors, three secretaries or acting secretaries of defense, and three chiefs of staff. In addition, there are numerous examples, including the resignation of Secretary of Defense Jim Mattis over the president's sudden surprise announcement that U.S. forces would be withdrawing from Syria, that suggest the president's foreign policy has been more erratic than strategic, lacking in both consistency as well as anything resembling a well-functioning policymaking process. Mandel tackles the usual debate about

[1] Kathryn Dunn Tenpas, "Why is Trump's Staff Turnover Higher than the 5 Most Recent Presidents?" *Brookings Institution*, 19 January 2018, https://www.brookings.edu/research/why-is-trumps-staff-turnover-higher-than-the-5-most-recent-presidents/.

whether the president actually has core foreign policy beliefs or shifting ones. But he fails to consider the role that the foreign policymaking process—or the lack of it—plays.

The Brexit case study is equally problematic, for different reasons. It makes no mention of the possibility that the referendum may have been influenced by foreign interference. Instead it argues that the Brexit vote resulted solely from domestic activities to harness the new information environment, even though two UK investigations into Russian activities have been opened (a Parliamentary investigation found evidence of Russian influence operations[2] while a National Crime Agency criminal investigation is still ongoing),[3] the Atlantic Council has called for further examination of potential Russian financing of domestic pro-Brexit groups now that the EU withdrawal process has been delayed[4], and the magnitude of Russia's information warfare operations in the United States during the 2016 presidential election has only grown over time, with new information unearthed by nonpartisan studies commissioned by the Senate Select Committee on Intelligence.[5] Mandel writes that his Brexit case shows how "in this age of the Internet and social media, bottom-up digital communication can match and in many circumstances outclass top-down state efforts in actually getting through to and influencing target constituencies," (74). But given the emerging evidence of Russia's top-down influence operations in the UK referendum and elsewhere, this conclusion is not terribly likely to hold up well.

The author's 9/11 case study emphasizes al-Qaeda's use of stealth, deception, and denial (129-130) and notes the difficulty of finding signals of real danger amidst so much noise. Here, too, a deeper examination of the facts suggests the argument is not nearly as strong or as well supported as Mandel claims.

At least two of the nineteen al Qaeda hijackers were not known for being particularly stealthy or deceptive. They were hiding in plain sight, using their true names on rental agreements, credit cards, bank accounts, travel documents, and even the San Diego telephone directory. They were also operating right under the FBI's nose, living for a time with an FBI informant, and making contact with several targets of past and ongoing FBI counterterrorism investigations over a period of months—all unknown to the FBI before 9/11. Contrary to Mandel's argument, these were not savvy terrorists using sophisticated tradecraft to evade U.S. intelligence abroad and at home.

What's more, the bigger lesson from 9/11 is not that signals are hard to find in the new information age. It's that even when signals are found, they often do not lead to success because organizational weaknesses get in the way. The FBI's New York Field Office started desperately hunting for these two hijackers nineteen days before 9/11, but the manhunt was limited to a single field office, given the lowest priority, and handed to an agent who had just finished his rookie year. The manhunt failed not because the hijackers were hard to find but because the FBI was not designed well to find them. All FBI cases, even nationwide manhunts, were assigned to a single lead field office. All intelligence investigations to prevent future disasters were considered lower priority than law enforcement investigations of past crimes. And finding a potential terrorist was

[2] House of Commons, Digital, Culture, Media and Sport Committee, "Disinformation and 'fake news': Final Report," Eighth Report of Session 2017-19, House of Commons HC 2791, 18 February 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. See also Mary Louise Kelley, " All Things Considered," National Public Radio, 12 July 2018, https://www.npr.org/2018/07/12/628546565/much-like-the-u-s-the-u-k-is-investigating-russian-meddling-in-its-politics.

[3] Robert Wright and Cynthia O'Murchu, "Crime Agency Investigates Arron Banks over Leave.EU Electoral Spending," *Financial Times*, 1 November 2018 https://www.ft.com/content/2401bf9a-ddd1-11e8-8f50-cbae5495d92b.

[4] Josh Rudolph, "Use Brexit Delay to Investigate Russian Money," *New Atlanticist* (blog), *The Atlantic Council,* 15 March 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/use-brexit-delay-to-investigate-russian-money.

[5] Senate Select Committee on Intelligence Press Release, 17 December 2018, "New Reports Shed Light on Internet Research Agency's Social Media Tactics," https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency%E2%80%99s-social-media-tactics.

considered the lowest possible job, which is why it was given to one of the least experienced agents. On the night of 9/11, an anguished FBI agent submitted the name of hijacker Khalid al-Mihdhar to the bureau's information technology center to see what a search of public records would uncover. Within hours, the agent received al-Mihdhar's correct address in San Diego.[6]

The manhunt was one of 23 opportunities that the CIA and FBI had to penetrate the 9/11 plot before disaster struck. Both agencies failed to capitalize on all 23 not because the information environment was too noisy but because their own agencies were too hidebound by Cold War structures, cultures, and incentives designed for a different time and a different enemy. While it's certainly true that the signals-to-noise ratio is a daunting and growing challenge in today's information age, 9/11 shows that signals can still be found, and that finding them is only half the battle.

Unfortunately, *Global Data Shock* promises more than it delivers. In addition to the analytic and empirical shortcomings in the case studies, the book tends to make sweeping assertions that are poorly supported by evidence. On page 16, for example, Mandel writes that, "Even when people are comfortable with technology, the information explosion can…reduce the ability of those most vulnerable to quickly adapt to changing conditions or to take appropriate steps to safeguard what is rightfully theirs" (16). How exactly do we know this to be true? We don't. And in fact, from the World Food Programme's use of satellite imagery and mobile phones to improve food security[7] to the use of text messaging by bombing and earthquake victims,[8] evidence suggests that technology has in fact *improved* the ability to assist vulnerable populations in natural disasters and manmade conflicts. Similarly, Mandel later writes that core powers today cannot set international rules of the game like the powers of yesteryear in part because they lack "universally recognized global legitimacy" (32). This statement suggests a) that universally recognized global legitimacy for great powers, whatever that means, actually exists; b) that great powers of the past had it but great powers of the present do not; and c) that international rules of the game are created and followed when globally legitimate powers make them. Few international relations scholars would agree with any of those claims.

"The search for meaning," writes Mandel, "is a universal human pastime" (195). *Global Data Shock* tackles an important set of issues in a new information environment, but the search for meaning continues.

[6] Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007).

[7] Shelley Thakral, "Technology in Emergencies Gives us the Bigger Picture. It Helps us Find Solutions," *World Food Programme Insight* (blog), *World Food Programme*, 20 August 2018, https://insight.wfp.org/technology-in-emergencies-gives-us-the-bigger-picture-it-helps-us-find-solutions-99670e92923e.

[8] Jacob Korenblum, "Mobile Phones and Crisis Zones: How Text Messaging Can Help Streamline Humanitarian aid Delivery," *Humanitarian Exchange* (magazine), *Overseas Development Institute,* March 2012, https://odihpn.org/magazine/mobile-phones-and-crisis-zones-how-text-messaging-can-help-streamline-humanitarian-aid-delivery/.

Response by Robert Mandel, Lewis & Clark

My primary purpose in writing this book was to stimulate spirited discussion about how the growing flood of data in the twenty-first century has the capacity under certain identified circumstances to enhance global propensities and capabilities to engage in manipulation, specifically strategic ambiguity, strategic deception, and strategic surprise. I acknowledged that this would not have been possible without the excellent work on international strategic manipulation that was written decades ago, but these invaluable insights clearly needed significant updating and reconsideration in light of the changing global information environment. While the reactions of the reviewers to the book are predictably mixed, I am absolutely thrilled that this vital discussion has begun, and I wish to thank Austin Carson, Kathleen Vogel, and Amy Zegart for taking the time to participate in this dialogue.

Although Zegart dismissively contends that the book's entire argument can be summed up in the obvious and trite phrase "more information is not always better," that ignores the work's most important contribution, which is to begin the important process of determining exactly under what conditions in today's world (1) information overload increases this global manipulation capacity and (2) the ensuing strategic ambiguity, deception, and surprise prove to be most dangerous from a security perspective. While the study's findings are explicitly identified as more tentative than definitive, such conditional analysis is unquestionably a key prerequisite to sound manipulation management—both offensive and defensive—in today's world. Contrary to Zegart's claim that the book is full of "sweeping assertions that are poorly supported by evidence," in fact it makes every attempt, using the case studies, to qualify the often blanket claims within the existing literature about information overload and strategic manipulation. For example, Zegart criticizes the book's statement that information overload *can* reduce the adaptive capacity of vulnerable targets as overly sweeping, but that statement is carefully qualified elsewhere in the volume. Moreover, while the book does claim that today great powers cannot set international rules of the game, a statement that is supported by virtually every major international relations analyst, it never sweepingly implies, as Zegart suggests, that they had the complete ability to do so in the past. Several major global order studies have mentioned that current great power global control has deteriorated over time.

The case studies are designed to be illustrative, and thus cannot serve a basis for rigorously proving or disproving hypotheses, in part because the book recognizes that the relevant publicly available evidence is often indirect and spotty. However, given some case-study questions that the reviewers raise, a response is warranted. Regarding the Donald Trump case study, every outside analyst agrees that President Trump's policies have been inconsistent and unpredictable and have served to create massive ambiguity about his actions in the minds of both targets and observers. When that reality is combined with Trump's repeated declarations that unpredictability is his intended policy, as opposed to that of his predecessor, Barack Obama, how crucial is it for this study to try to decisively determine (per Zegart's and Carson's suggestions) whether these policies might alternatively result from bureaucratic weakness or incompetence/impulsiveness? The significant turnover in high-level personnel in the Trump administration is not, as suggested, inherent proof that his behavior is erratic, for that could be part of a plan to keep everyone guessing and avoid accountability for his actions; Zegart's notion of a "well-functioning" policy process is not one that is necessarily consistent with an unrelenting desire to maximize unpredictability.

Turning to the Brexit case, the extent to which foreign influence heavily influenced the outcome of the referendum is still under considerable debate, and my careful reading of the evidence suggests that Zegart's objection to my more domestically-focused interpretation exaggerates the role of Russian influence, as is vividly demonstrated by the very recent overwhelming British popular vote in support of Prime Minister Boris Johnson's conservative pro-Brexit stance without any trace of significant Russian manipulation. Moving to the 2003 Iraq case, it seems difficult to argue with certainty, as Carson does, that the Weapons of Mass Destruction (WMD) verification issue was largely a problem of data scarcity rather than data overabundance: if more information from inspectors had been available during the very limited time period when inspection occurred, could not questions and differing opinions have mushroomed about whether deeply hidden sites were still missed or whether the traces found were indisputably linked to nuclear weapons rather than to other uses? As the book argues, more information can certainly in many instances clarify, but it can also give rise to more debate, especially when source credibility is not taken for granted and when the quality, quantity, and key players' differing interpretations of information (all of which the volume explicitly analyzes) are considered.

Finally, as to the case of the 9/11 attacks, the book does not claim, as Zegart suggests, that every terrorist was savvy and sophisticated; its primary point is rather that the plan itself used deception in a clever manner. Moreover, I would strongly argue, in contrast to her argument, that responding to signals once they are correctly found is itself directly complicated by the sea of other signals, correct and incorrect, relevant and irrelevant, that are present at the same time about different dimensions of an adversary's behavior. One should not completely separate the act of distinguishing true from false signals from that of determining what to do in response to discovered signals, for to do so could easily lead to overly compartmentalized signal interpretation.

A key issue raised by Carson is whether strategic manipulation was any different on a global level prior to today's digital age and the resultant overwhelming flood of data. In the book's first chapter, I attempt to begin to answer that question by analyzing how the current data predicament might have affected the 1973 Yom Kippur War, which occurred well before the Internet age and which is famous for involving strategic ambiguity, deception, and surprise. Certainly the current information interpretation and strategic manipulation predicament is not unique, but the book argues that the security challenges have dramatically intensified.

Lest my comments here be perceived as overly defensive, let me give praise for some really perceptive reviewer remarks. Vogel is truly incisive at noting within intelligence work the central contaminating influence of many fixed analytical frames in evaluating the wealth of information gathered, and she rightly points out that that the intelligence community's eagerness to embrace big data and artificial intelligence technologies has often come without sufficient attention to the human-centered challenges of working with and trusting such systems. Carson provides trenchant and useful future research ideas. First, as he notes, one of this volume's key limitations is that it does not systematically analyze the relative causal weight of information overload compared to other explanations of emerging patterns. Data glut is certainly not the exclusive stimulant here, despite its significant impact in each case. Although I considered dealing with its relative value, I felt it was beyond the scope of this book, and follow-up investigations should indeed pursue this valuable line of inquiry. Second, as Carson confirms, the issue of credibility is at the heart of this volume's policy implications, which suggests the need for follow-up studies to explore in more detail the means for credibly combating "dubious disinformation campaigns." Third, in a closely-related manner, while the book provides some hints about when and how "cohesive political responses" to strategic ambiguity, deception, and surprise are most necessary and possible, more follow-up work would also be useful here as well. My sincere hope is that in the future *Global Data Shock* contributes to more refined, focused, and collaborative dialogue not only about aiding the search for meaning but also about discovering a myriad of ways to improve global intelligence-gathering, data science, signaling, and message verification.