Article

Science, Technology, & Human Values
2017, Vol. 42(6) 1061-1099

DOI: 10.1177/0162243917727353
journals.sagepub.com/home/sth
SAGE

Target Practice: Counterterrorism and the Amplification of Data Friction

Jon R. Lindsay[1]

Abstract

The nineteenth-century strategist Carl von Clausewitz describes "fog" and "friction" as fundamental features of war. Military leverage of sophisticated information technology in the twenty-first century has improved some tactical operations but has not lifted the fog of war, in part, because the means for reducing uncertainty create new forms of it. Drawing on active duty experience with an American special operations task force in Western Iraq from 2007 to 2008, this article traces the targeting processes used to "find, fix, and finish" alleged insurgents. In this case they did not clarify the political reality of Anbar province but rather reinforced a parochial worldview informed by the Naval Special Warfare community. The unit focused on the performance of "direct action" raids during a period in which "indirect action" engagement with the local population was arguably more appropriate for the strategic circumstances. The concept of "data friction", therefore, can be understood not simply as a form of resistance within a sociotechnical system but also as a form of traction

[1]University of Toronto, Toronto, Ontario, Canada

Corresponding Author:
Jon R. Lindsay, University of Toronto, 315 Bloor Street West, Toronto, Ontario, Canada M5S 0A7.
Email: jon.lindsay@utoronto.ca

that enables practitioners to construct representations of the world that amplify their own biases.

Keywords
engagement, intervention, politics, power, governance, methodologies, methods, epistemology, other

Introduction

In a famous passage of *On War*, Clausewitz walks the novice onto the battlefield. From "the slope where the commanding general is stationed with his large staff," he leads us through mounting danger and fear to "the firing line, where the infantry endures the hammering for hours" (Clausewitz 1976, 113). On a trip to a modern combat zone, one finds staff officers hammering away at keyboards and enduring video teleconferences for hours, with only a small minority of personnel firing at anything at all. A trip to Iraq in 2007 is better narrated in reverse.

Our helicopter ferries troops, reporters, and supply pallets through the desert, occasionally maneuvering and ejecting flares into the night in response to what could either be a surface to air threat or just stray electronic emissions. Once we arrive "inside the wire" of the forward operating base and settle onto the airstrip, we gather up our kit and shuffle through the rotor wash to a squat wooden hut, where a young marine checks our identification. A minivan picks us up and drives us past contracted military guards standing around barrel fires, silent artillery pits, and tank parks. The road changes from dirt to asphalt as we drive deeper into the base, with all the conventional paraphernalia of road signs, traffic police, coffee shops, and convenience stores. We eventually pull into the headquarters of a special operations task force (SOTF, pronounced sō'-tif), a base within a base surrounded by blast walls and gabions that enclose a collection of monster trucks, unmarked civilian vehicles, and a bunch of men working out. We enter a complex of air-conditioned Alaskan Shelters and stow our body armor and weapons in cubbyholes next to an impressive pantry of junk food and energy drinks. Several rows of bored civilians and sailors in T-shirts, many with shaggy hair and mustaches that contrast with the clean-cut marines outside the SOTF, sit in front of their laptops, chat on the phone, joke with each another, watch Fox News on the television, or gaze at drone video projected on the wall, which shows nothing in particular happening in some suburban neighborhood. They describe themselves as

"staff bitches," who do paperwork rather than participate in more heroic operations "outside the wire." The desks in this expeditionary office space are covered with computer monitors, stacks of papers, family mementos, and humorous kitsch, and the next building over has a video-teleconference room with comfortable chairs. Someone is yelling at his e-mail because a *PowerPoint* file is taking too long to send.

This article presents an autoethnography (Anderson 2006) of what I call *epistemic infrastructure*, the network of practices and equipment that constrain and enable an organization's ability to understand its environment (Hutchins 1995; Orlikowski 2000; Mindell 2002). From 2007 to 2008, I mobilized to active duty from the US Naval Reserve and served with a SOTF in Western Iraq. I had the opportunity to participate in and observe the ways in which people used digital technology to make sense of their war, a practice simultaneously more mundane and more fraught than generally appreciated. This study draws on personal observations from the SOTF headquarters of over 200 raids resulting in the capture of over 300 detainees over the course of a six-month deployment. I describe the recurrent behavioral patterns that enabled the SOTF to represent and "kill or capture" its targets, exploring the ways in which cultural identities shaped technological processes. It was not possible to measure the specific effects of the raids conducted on the political situation that justified them; indeed, the inability or unwillingness of a self-insulated information system to assess its own effectiveness is one important finding of this study.

In this case, I find that epistemic infrastructure amplified the preferences of the Naval Special Warfare community rather than clarified the social reality of Anbar Province. The SOTF had no one centralized panopticon to make sense of its world comparable to the air defense plot in the "closed world" of a nuclear command center (Edwards 1996). Across its multiple computer workstations, and in multiple applications on individual workstations, computer users freely modified and copied digital files to organize their local views of operational reality. Usually, they did not or could not articulate all of the assumptions that guided their interventions, and they discarded or lost track of data provenance along the way. The SOTF's digital infrastructure exerted a decentering effect across the archipelago of camps along the Euphrates and even among personnel working in the same room. Information practice at the SOTF was beset by "data friction" at the intersection of "data surfaces" not unlike the situation Edwards (2010) describes in global climate science. The mechanical metaphor of friction suggests a form of resistance that prevents an

organization from achieving its goal. In this case, however, data friction made it *more* likely that the SOTF would achieve objectives informed by the culture of Naval Special Warfare. Pervasive data friction in the construction of representations of the world necessitated continuous accommodation and repair that tended to reinforce a parochial worldview that emphasized "direct action" raids over "indirect action" engagement with the local population.

This article begins by framing the conceptual problem of data friction in a military context. I then describe the historical context for SOTF operations in 2007-2008 and my methods for studying them and the data practices that enabled the organization to "find, fix, and finish" its targets. I conclude with a general discussion of the implications of friction for military counterterrorism operations.

Data Friction and the Fog of War

Clausewitz (1976) observes that "three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty" (p. 101). Amid the millennial excitement about the information age of the 1990s (Lawson 2014), military officers wrote books with titles like *Lifting the Fog of War*, imagining that "technology can give us the ability to see a 'battlefield' as large as Iraq…with unprecedented fidelity, comprehension, and timeliness" (Owens and Offley 2000, 15). Despite the technocratic optimism, uncertainty was endemic in Iraq, and the US military struggled to adjust ideas about "network centric warfare" to a foggier reality (Ferris 2004; Biddle 2007; Shimko 2010; Lindsay 2013). Numerous critics have lambasted visions of better fighting through information technology, affirming the Clausewitzian nature of war as a "paradoxical trinity" of political reason, elemental violence, and random chance (Beyerchen 1992; Van Riper 1997; Harknett 2000; McMaster 2003; Watts 2004). Indeed, as Clausewitz (1976) points out,

> Everything in war is very simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war…. Countless minor incidents—the kind you can never really foresee—combine to lower the general level of performance so that one always falls short of the intended goal…. Friction is the only concept that more or less corresponds to the factors that distinguish real war from war on paper. (p. 119)

Clausewitz mobilizes the notion of friction to describe resistance arising within a military organization, which he likens to a machine: "when much is at stake, things no longer run like a well-oiled machine. The machine itself begins to resist" (p. 104). The sources of friction enumerated in *On War* include "danger, exertion, uncertainty, and chance" (p. 104). Modern standoff weapons appear to reduce danger, at least for the people aiming them. Office work appears to reduce physical exertion, although staff officers are often sleep deprived. Sophisticated intelligence sources and methods appear to improve information, yet they rely on a complicated, bureaucratic, and global sociotechnical infrastructure that expands the play of chance. The very means adopted for reducing uncertainty themselves become new sources of uncertainty.

While Clausewitz offers a rich and pragmatically grounded account of war (Sumida 2008), his account of technology is historically circumscribed. In the Napoleonic era, Clausewitz might reasonably argue that "strategy uses maps without worrying about trigonometric surveys" (p. 144), but military practitioners today spend a lot of time worrying about the sociotechnical construction of the "common operational picture" that mediates their knowledge of the world. Clausewitz describes activities like "building roads and bridges," even "in full view of the enemy," as "merely preconditions" to the engagement, asserting that "essentially these activities are alien to the conduct of war…so far as *their actual construction* is concerned" (p. 130).[1] Clausewitz insists, however, that "To the extent that *regulations* and *methods* have been drilled into troops as active principles, theoretical preparations for war are part of its actual conduct…. [T]hey are accepted as given procedures and as such must have their place in the theory of the conduct of war" (p. 152). Today the algorithms in guided munitions and the software protocols in analytical tool kits are, in a very real sense, "drilled in" to military organizations "as active principles." Information technologies act as epistemic prosthetics to extend the human mind (Hutchins 1995; A. Clark and Chalmers 1998; Sterelny 2004; Noë 2009). Materially imbricated assumptions shape organizational understandings (Vaughan 1996; Bowker and Star 1999; Snook 2000; Eden 2004), and screens, controls, networks, and bureaucracies mediate human experience of modern war (Virilio 1989; Edwards 1996; Mindell 2002; Der Derian 2009; Wolters 2013). Clausewitz argues, "One would not want to consider the whole business of maintenance and administration as part of the *actual conduct of war*" (p. 129). Yet today, the technological "nonhumans" (Latour 1992) that constrain military knowing and acting are vital in "the *actual conduct of war.*"

Edwards's (2010) notion of "data friction" helps to bridge the technology gap that Clausewitz leaves open. While Edwards does not explicitly cite the Prussian strategist, he does include a chapter on "data wars," addressing the politicization of climate science, in which the construct of friction is key. Because "data always have a material aspect," Edwards writes, there are "costs in time, energy, and attention required simply to collect, check, store, move, receive, and access data" (p. 84). Friction is the resistance encountered whenever "dissimilar data surfaces make contact. Some of those surfaces are human; they make mistakes, argue, and negotiate. Every interface slows you down and eats up energy. All that friction generates error and noise" (p. 97). Edwards distinguishes "data friction" from "computational friction," which "expresses the struggle involved in transforming data into information and knowledge," and he emphasizes that "data friction expresses a more primitive form of resistance" because data can be embodied in material other than computer memory (p. 84). He further distinguishes metadata friction, "the difficulty of recovering contextual knowledge about old records" (p. xvii). The particular format of data is always a result of particular decisions made in circumstances that may be hard to discern or deliberately obfuscated, distorted, or withheld. Science is often hotly contested (Jasanoff 1987; Hackett 2005), although usually not as violently as in war. At the same time, the expanding role of information work has created a more civilianized, office-like experience for a growing proportion of military practitioners (Janowitz 1959; Ferris and Handel 1995). Just as "the making, maintaining, and modification of scientific knowledge is a local and a mundane affair" (Shapin 1995, 303), war is also more "littered by endless minor obstacles than…great, momentous questions" (Clausewitz 1976, 120). The minor obstacles to battlefield performance increasingly include data frictions not unlike those that Edwards finds in climate science.

The Clausewitzian emollient for friction is "genius," which encompasses both determination under fire and "*a sense of locality.* It is the faculty of *quickly and accurately grasping the topography of any area* which enables a man to find his way about at any time. Obviously this is an act of the imagination" (p. 109). Local material circumstances provide resources for improvisation that enable practitioners to try out new approaches. Active sensemaking and collaborative repair are prominent phenomena in most sociotechnical systems, especially with readily reconfigurable digital technologies (Ihde 1990; Dreyfus 1991; Weick 1995; Orlikowski 2000; Ciborra 2002; Oudshoorn and Pinch 2003; Suchman 2007). Friction, which emerges in the idiosyncratic intersection of particular data

surfaces and different social communities, is thus not only a problem but also a source of traction for intergroup communication and adaptation (Tsing 2005; Edwards et al. 2011). Bottom-up user innovation has been found to enhance military performance by fielding novel capabilities, adaptive responses to unforeseen developments, or working around unresponsive bureaucracies (Weick and Roberts 1993; Carafano 2006; Lindsay 2010; Russell 2011; Kollars 2014). This study confirms the importance of performative repair in military settings, which is usually celebrated, but further explores some less genial aspects. Data friction and user responses to it have the potential to generate additional friction for other users and to lock in counterproductive organizational understandings and behaviors. The meanings that emerge through epistemic infrastructure are socially produced to be sure. Yet even an ostensibly uniform society like the military includes many different groups that tussle with each other or operate with some degree of independence. When data processes become captured or corrupted by one particular subculture, the results can have deleterious consequences for others affected by them. This includes members of the warfighting organization, who must struggle with breakdowns in their epistemic prosthetics, as well as people in the local population, who must suffer the consequences of equivocal targeting. Repeated targeting errors can increase the human costs of war, relieve pressure on the administrative and logistical core of the insurgency, and enhance support for insurgents by generating resentment for counterinsurgents, thereby contributing to the protraction of the conflict. Data friction and misguided genius can amplify these pathologies.

A note on acronyms (Table 1). The nomenclatures of war and computer science abound with acronyms, so their intersection in military information systems is especially dense. I once overheard someone ask, "Did you PID that POL this POD?" They meant, did you receive any intelligence intercepts providing "positive identification" (PID) of your analysis of a target individual's "pattern of life" (POL) during our environmental window for operations this evening, that is, "period of darkness" (POD)? The wealth of neologism in military culture reflects its complex dynamic milieu. Acronyms provide a shorthand to economize in communicating specific distinctions in fluid circumstances, and they orient attention to the emergence of new reconfigurations and combinations of processes, systems, missions, and organizations. Yet they also become linguistic markers of subcultures that can be incomprehensible to outsiders. Indeed, acronyms are both a response to and another source of data friction.

Table 1. Acronyms.

AQI	Al-Qaeda in Iraq
COIN	Counterinsurgency
CONOPS	Concept of operations
CONUS	Continental United States
F3EA	Find, fix, finish, exploit, and analyze
FOB	Forward operating base
GIS	Geospatial Information Program
HUMINT	Human intelligence
ISIS	Islamic State in Iraq and Syria
ISR	Intelligence, surveillance, and reconnaissance
JAG	Judge advocate general
JSOC	Joint Special Operations Command
MEF	Marine expeditionary force
OPSUM	Operations summary
PID	Positive identification
POD	Period of darkness
POL	Pattern of life
PUC	Person under control
RFI	Request for information
ROE	Rules of engagement
SCI	Sensitive compartmented information
SEAL	Navy "sea, air, and land" special operator
SIGINT	Signals intelligence
SIPRNET	Secret Internet Protocol Routing Network
SOF	Special operations forces
SOTF	Special Operations Task Force
TIP	Target intelligence package
TOC	Tactical operations center

Tribal Engagement

I served on the SOTF headquarters staff as the "nonlethal effects officer" responsible for coordinating "tribal engagement," civil affairs initiatives, and some intelligence activities. This position sensitized me to the complex local politics in Anbar, which had just emerged from several years of brutal violence and was in the process of rebuilding. In June 2006, a classified report assessed that Coalition Forces "are no longer capable of militarily defeating the insurgency in al Anbar" (Ricks 2009, 339-43), but a year and a half later, violence had dropped to the lowest levels since the beginning of the war.

Explanations for this surprising turnaround remain contested, and different regions of Iraq experienced quite different dynamics (Lindsay and

Petersen 2012; Hagan et al. 2013). An initial wave of American accounts credited counterinsurgency (COIN) doctrine that prioritized protecting the population over hunting the enemy (Smith and MacFarland 2008; Searle 2008; Michaels 2010; Biddle, Friedman, and Shapiro 2012; Green and Mullen III 2014). General David Petraeus, the commander of Coalition Forces during the "surge" of additional American troops to Iraq, championed COIN in public. His new field manual (US Army 2006, 1-29) included a table of "Unsuccessful practices" that included points such as "Overemphasize killing and capturing the enemy rather than securing and engaging the populace" and "Focus special forces primarily on raiding." Yet in the shadows, Joint Special Operations Command (JSOC) conducted a counterterrorism campaign that focused special forces exclusively on raiding. Operating at a relentless pace with the collaboration of US national intelligence agencies, JSOC removed as many as 12,000 alleged insurgents from the battlefield between 2003 and 2008, killing perhaps a third (Urban 2011, 270-71). Many have credited JSOC with crippling the Sunni insurgency in Iraq (Woodward 2008; Ambinder and Brady 2012; Naylor 2015). Others point out that the culmination of the sectarian civil war resulted in the de facto separation of Sunni and Shia just as surge troops arrived (Parker and Hamdani 2006; Rosen 2009). In Sunni-dominated Anbar, moreover, the violence plummeted well before the troop surge. Anbari tribes that once had resisted the occupation decided to approach Coalition Forces for help in ejecting Al-Qaeda in Iraq (AQI, known today as the Islamic State or ISIS), in essence realigning with the lesser of two evils (Long 2008; McCary 2009). Scholarship drawing on Iraqi perspectives (Montgomery and McWilliams 2009; al-Jabouri and Jensen 2010; Jensen 2014; Cottam, Huseby, and Baltodano 2016) emphasizes the importance of Iraqi agency in initiating the "Anbar Awakening" as well as the underappreciated role of local vigilantes in exterminating Al-Qaeda members, both of which are at odds with triumphalist American accounts. That the historiography today of a pacification episode a decade ago remains so unsettled is itself evidence that contemporaries had difficulty understanding what kind of war they were fighting.

My "tribal engagement" job title referred to coordination with the Bedouin chieftains who determined Anbari politics, but in practice, I spent more time engaging with the internal tribes of the SOTF. I tried, often unsuccessfully, to make the case that "nonkinetic" missions emphasizing communication, development, and intelligence collection might be better for long-term stability than "kinetic" missions that accorded more with the commando identity of the Naval Special Warfare community. US Navy

SEALs have attained a near-mythological status in popular culture, exemplified by recent films such as *Zero Dark Thirty*, *Lone Survivor*, and *American Sniper*, all based on swaggering autobiographies or hagiographies.[2] The same SOTF described in this article has received a heroic, and heroically biased, chronicling of its combat operations from 2005 to early 2007 (Couch 2013). Yet there are real questions whether the SOTF made much of a difference during that time given the concurrent Anbar Awakening and marine COIN campaign. By Couch's own account, SEAL snipers in 2006 tended to attract insurgent attacks, so the SEALs had to be withdrawn as commanders realized that the excess fighting had become counterproductive for the ostensible mission of protecting US troops.

Military jargon tends to describe missions that involve communication and negotiation in negative terms, as nonkinetic, nonlethal, nontraditional, indirect, unconventional, or other than war. Military culture tends to resist indirect missions like COIN in favor of more traditional combat missions, and durable military subcultures shape the ways in which different units conduct COIN when it becomes a functional necessity (Jackson 2008; Long 2016). The Naval Special Warfare community in particular has a pronounced preference for "direct action" missions to kill or capture enemy combatants, while neglecting "indirect action" missions such as engagement with local elites, partner force training, psychological (information) operations, and civil affairs development initiatives that work "by, with, and through" the local population. One prominent senior SEAL penned a "theory of special operations" that included no treatment whatsoever of indirect missions (McRaven 1995). A gendered interpretation is suggestive. High-status SEAL "operators" were exclusively men, but women (and men) could serve as lower-status "techs" to provide administrative, intelligence, communications, medical, and logistics support. Operators sought the glory of direct action, while indirect action was left to techs and reservists. Operators received extensive training for eighteen months prior to the deployment, but most techs arrived just prior to deployment with uneven skills. Yet the SOTF had twice as many techs as operators, and many SEAL-qualified individuals were in fact employed in staff positions. As a result, information technology and knowledge management savvy were quite unevenly distributed compared to tactical proficiency for direct action. Information work, including intelligence analysis and computer network operations, can reasonably be described as indirect work as well, since data can only affect the battlefield when people or machines translate them into direct effects. Naval Special Warfare thus had a double bias against indirect action, first in its preference

for conducting raids over other COIN missions and second in its haphazard information work for any mission whatsoever.

By late 2007, in any case, Al-Qaeda had been largely displaced from the province and the overall coalition emphasis had shifted to political stabilization, economic development, and preparation for the peaceful transfer of power to Iraqi authority. The SOTF was a battalion-sized organization of approximately 400 people. A much larger marine expeditionary force (approximately 30,000 people) was the "battlespace owner" responsible for implementing coalition strategy in the province, and in 2007-2008, the marines emphasized security and reconstruction for the local populace in an effort to demobilize tribal militias and bolster the legitimacy of the Iraqi government (Shultz 2013). Marines provided basing and emergency response services for the SOTF, and coordination with the marines was a practical necessity, but the SOTF was part of a separate chain of command for special operations that gave it the authority to select its own missions. The idea was that "silent professionals" worked best if local commanders had the freedom to judge the situation and act accordingly within the scope of their headquarters' intent, but problems might emerge if they failed to act silently or professionally. SOTF priorities seemed disconnected from the strategic environment, but the organization had enough autonomy to pursue them nonetheless.

My official duties afforded me the opportunity to visit military bases and Iraqi towns along the Euphrates river valley and to trace data practice throughout the organization. There was a natural synergy between participation and observation, given my interest in epistemic infrastructure. Conversations about data management and organizational processes would have occurred even in the absence of any research agenda (Schultze 2000; Forsythe 2001). Military officers have to continuously repair breakdowns in the complex technologies that mediate their knowledge of the battlefield, which entails alternating attention between what information means and how information works. I was open with military colleagues about my civilian identity as an academic researcher, but standard ethnographic methods such as recording were infeasible, given wartime duties and classified workspaces. Conveniently, formal classification guidelines cover explicitly enumerated bureaucratic processes, capabilities, and arrangements (Galison 2010), while informal information practices tend to be overlooked. Accordingly, routine classification review of this material resulted in no redaction. A disadvantage of my approach is that I must omit detail about specific operations and intelligence methodologies that remain classified. The compensating advantage is that I can cast some light on the interpretive behavior that made those operations possible.

I am obliged to say that my opinions do not reflect those of the US government, but my critical findings should make this obvious. Other accounts of special operations based on insider access tend to be overly admiring (Simons 1997; Robinson 2004), focused on battlefield reportage (Naylor 2005, 2015; Urban 2011), or preoccupied with professional questions of force structure and employment (Rothstein 2006; Andres, Wills, and Griffith 2006; Tucker and Lamb 2007). I do not pretend to provide a definitive assessment of US counterterrorism in Iraq or elsewhere. My focus here is on the implementation of targeting by one particular tactical unit and its endogenous creation of data friction.

Target Practice

The SOTF was just one of many special operations units in Iraq. The "special mission units" affiliated with JSOC are sometimes described as "black SOF" (special operations forces) because their identities are protected by cover names, and they operate under special authorities at the "national" level of command (Tucker and Lamb 2007; Naylor 2015). The SOTF, by contrast, was a "white SOF" unit that operated discretely but overtly at the "theater" level of command, yet still separately from the marines in Anbar. The SOTF's mission nominally included Iraqi training and engagement missions in close coordination with the marines, but SOTF operators aspired to conduct unilateral counterterrorism operations in the manner of JSOC, despite having far fewer resources than JSOC.

Emulating JSOC meant emulating the "find, fix, finish, exploit, and analyze" (F3EA) targeting doctrine developed by Lieutenant General Stanley McChrystal and his intelligence director Colonel Michael Flynn (Flynn, Juergens, and Cantrell 2008; US Army 2015). F3EA or "counter-network operations" aimed to use intelligence to improve raids and raids to improve intelligence. Technical intelligence and human sources identified and located suspected insurgents, while detainee interrogation and analysis of captured documents fed intelligence back into the system. In theory, the F3EA cycle made an invisible network visible by using continuous raids and data recovery to recursively iterate through the underground organization, from soldiers to lieutenants to commanders, thereby disrupting the insurgency faster than it could regenerate. F3EA built on earlier military and policing methods described variously as "manhunting," "decapitation," or "countergang" operations, but in Iraq JSOC generated such a high volume and pace of operations that practitioners described it as "industrial counterterrorism." McChrystal appropriated the slogan, "It takes

a network to defeat a network," to stress the vital organizational dimension of this innovation (McChrystal 2013, 148; Lamb and Munsing 2011). As General Petraeus observed, "There have been breakthroughs in the disciplines of human intelligence (HUMINT), signals intelligence, imagery intelligence [and] measurement intelligence…and each is supported by the proliferation of computer applications, intelligence platforms and growth in various capabilities…. But the real breakthrough has been in the fusion of all this…and in the coordination and cooperation of all elements" (Naylor 2008). Whether or not JSOC ever actually achieved this ideal, the SOTF fell quite short of it.

Targeting Assumptions Structure Intelligence Collection

As Edwards (2010, 109) writes, "We speak of 'collecting' data as if they were apples or clams, but in fact we literally *make* data." Practitioners likewise speak of collecting "raw intelligence," but inscriptive processes are always based on interpretive choices (Räsänen and Nyce 2013). Errors in the fabrication of data may be random, but they can also be systematically biased if the actors involved have some particular interest in what gets collected and passed along.

Intelligence collection at the SOTF began when physical interactions with something in Iraq were transduced into material inscriptions or "immutable mobiles" (Latour 1987) that analysts could move, copy, and combine to make sense of the battlefield. Standardized reporting channels and formats delivered formal records of some sort of prior physical contact with external entities. Yet each processing step had the potential to discard provenance metadata or introduce spurious information. "Sanitization" practices intentionally stripped metadata from standardized reports to protect sensitive sources (e.g., disguising a telephone intercept as an agent report). Intelligence professionals with experience over a long career cultivate a feel for tradecraft and pitfalls in different collection disciplines (R. Johnston 2005; Fischhoff and Chauvin 2011), but analytical experience in the SOTF was uneven due to last-minute personnel augmentation and underinvestment in the training of "techs." Naval Special Warfare culture, moreover, tacitly encouraged techs to process intelligence under the assumption that it would eventually produce actionable targets rather than, say, an understanding of local politics.

As suggested in the opening vignette, SOTF personnel worked in a classified information environment protected by an elaborate infrastructure of bases, barbed wire, and controlled entry. The materiality of data afforded physical control. Highly classified inscriptions resided in a special room

called a "sensitive compartmented information facility" (SCIF). Cryptologic technicians, more gatekeepers than analysts, received signals intelligence (SIGINT) from sources at the national, theater, or unit ("organic") level. Sensitive SIGINT was "sanitized" before it was released to the rest of the SOTF to deliberately create ambiguity about the source of the intelligence, which inevitably stripped off provenance data. Some SOTF staff members, if they had the right clearances, made regular pilgrimages into the SCIF to hear the latest unsanitized news. Access to compartmented intelligence might provide knowledge but certainly conferred prestige to the in-group; the value of SIGINT was sometimes conflated with the height of the barriers protecting it.

Much of the recent scholarship on military drones (Strawser 2013; Bergen and Rothenberg 2014; Evangelista and Shue 2014; Horowitz, Kreps, and Fuhrmann 2016; Gusterson 2016) focuses on targeted killing, but the SOTF used drones exclusively for "intelligence, surveillance, and reconnaissance" (ISR). Drones collected over 200,000 hours of video in 2007 over both Iraq and Afghanistan, but at the SOTF, there was no automated way to find and catalog interesting results (Drew 2010; Shanker and Richtel 2011). SOTF personnel used a chat client on the classified Internet (Secret Internet Protocol Routing Network [SIPRNET]) to schedule collection missions through the higher headquarters in the neighboring province and communicate with drone operators a continent away. Sometimes chat room voyeurs clogged the circuits and inadvertently blocked legitimate users from reconnecting. SOTF analysts had to watch hours of video through the overhead sensor, which they described as "looking through a soda straw," for hours or days at a time while nothing out of the ordinary occurred as Iraqis went about their daily life. This boring task was often assigned to inexperienced junior personnel who were expected to store snippets of interesting video (in their judgment) on the Task Unit's share drive. They saved the files in folders named for whatever target was being monitored at the time (usually under some codename) and had no geographically tagged database of historical coverage; these data were as good as lost for future analysis by any different sorting scheme. These were seductively solvable engineering problems in principle, but the SOTF had neither the technical expertise nor agreement about common cataloging procedures to solve them. The "eye in the sky" blinked a lot, undermining the acuity of what practitioners described as the "persistent stare."

HUMINT, the oldest form of collection, offered a potentially valuable complement to technical collection (Hitz 2004; Innocenti, Martens, and

Soller 2009). The problem, widely recognized in the intelligence community, is that spies lie for a living. Informants might finger "terrorists" to liquidate personal grudges (Kalyvas 2006), fabricate stories to make money or enhance their status, play different HUMINT organizations of one another, or infiltrate as double agents to lure American troops into an ambush. HUMINT collectors might vet agents by cross-checking their reporting and asking them to perform nontrivial, observable tasks. However, SOTF collectors were recently retrained SEAL operators (as techs were less trusted outside the wire) with little professional experience (cf. Couch 2013, 40-41, 219-22). Their finished reporting was often vague and uncritical (e.g., "the man with a mustache wearing a *dishdasha* is a terrorist" could indict almost any Iraqi man). Collectors bristled at the suggestion that their informants might be out of their control ("My sources don't lie!"), discouraging doubts from those positioned as second-class techs. The SEALs queried their informants and focused their reporting narrowly on suspected targets rather than the political, economic, or tribal dynamics that might have improved understanding of the local mood or suggested indirect alternatives to direct action. Ironically, while they often discussed local politics and motivations for fighting (or defecting) in the course of vetting and establishing rapport with Iraqi sources, this information remained segregated in "source management" computer systems or was never recorded at all. Collectors believed that outsiders in their own organization had no need to know the political and personal backgrounds of their sources. They e-mailed their reports as Microsoft *Word* documents to avoid the cumbersome reporting bureaucracy of official HUMINT filing. Some collectors simply passed information along verbally to target hungry operators, leaving little trace for future analysis or auditing. The collectors' relaxed grooming standards, civilian clothes, segregated work spaces, and isolated computer systems inadvertently created barriers to collaboration and inhibited performance evaluation; more worrisome, the same skills that they honed to manipulate informants could also be directed against their colleagues.

Five years into the war in Iraq, most US personnel had little familiarity with the Arabic language, let alone the Iraqi dialect. The constant rotation of personnel, many of them reservists, made investment in language proficiency uneconomical compared to combat skills, adding to the impairment of indirect action missions and HUMINT that depended on intensive communication. Iraqi interpreters ("terps") were gatekeepers to linguistic access to the population and thus another source of inscriptive equivocation. Some collectors and interrogators even allowed their terps to run the meetings.

Iraqi names were transliterated inconsistently in reporting (e.g., "محمد" was rendered variously as "Mohammad," "Muhammad," or "Mohamed"), which complicated database searches. Intelligence organizations compensated by investing in automated translation systems and pattern-matching algorithms to link transliterations and naming variants rather than training people to speak Arabic.

In every pathway for collection, there were opportunities for human selection, or suppression, of some features over others. Only the sanitized results propagated downstream into further representations. Various computational transformations or manual cut-and-paste operations created potential for data equivocation and loss of provenance. Yet through all the noise, SOTF personnel still managed to find a signal, even if it was really just a reflection of their own assumptions. The commando organization was primed to look for targets and its collection was biased accordingly. Data potentially relevant to a deeper understanding of the social milieu dropped out as people stabilized the pathways that led to actionable targets.

The (Con)fusion of Operations and Intelligence

SOTF briefings to visitors evoked the mystique of "Ops–Intel fusion," but the phrase really underlined the persistent boundaries and confusion between work centers, and between processes dominated by higher-status operators or lower-status techs. The SOTF did not and could not have one master fusion system because there was no one common representational center, but rather a fragmented assemblage of partial and inconsistent representations. The fusion process was meant to combine multiple sources of intelligence to identify a "high-value individual" and discern his "pattern of life" to afford "fixing" the location where he (targets were almost always male) might be "actioned," which might then generate new intelligence according to the F3EA model. The representational genres in this process include network diagrams, target lists, and target packages.

Network diagrams could obscure as much as they revealed. Working analysts defined links and nodes incommensurably across different applications, parsing their local world into inconsistent types of entities, relationships, and characteristics (Bowker and Star 1999). One analyst included farm animals in the "person" category so he could track specific sheep that a shepherd was using to smuggle weapons. Analysts encoded information in the visual layout by drawing shapes around clusters of icons to indicate organizational affiliation, spacing icons closer or further apart to indicate the strength of a relationship, or using icons to represent intelligence reports

as well as the things those reports were about. Such data became inaccessible to graph–theoretical algorithms that operated only on links and nodes. Working diagrams served mnemonic and heuristic roles for analysts who monitored reporting on some specific circumscribed problem. The act of building a diagram forced analysts to read the reporting more closely, which made them smarter about their topic even if the diagram itself became illegible to anyone else. Insofar as the sensibility of these diagrams depended on the local interpretive expertise of analysts, their mobility as a useful inscription was limited even as the paper itself might be carried away (through classification boundaries erected to protect it). Such problems were lessened in cases where durable infrastructure such as engineered roads, telephone networks, or electronic transactions helped to standardize link and node ontology.

Impressive visualizations created an aura of professional expertise for techs in the eyes of operators. Social network diagrams hung as wall decorations long after the analysts who built them were gone and the insurgency evolved into something different. People described these charts as "hair balls" (because they were uselessly tangled) or "star charts" (because they plotted insurgent celebrities). Of course, the real insurgent networks continued to evolve as these diagrams were being constructed, and they could get out of sync. The hair balls appeared seductively detailed, but they hid assumptions and transcription errors in their methodologically fraught construction. Some individuals in Anbar played multiple roles in different social networks, defying easy categorization of people as "civilians" or "militants" (Wilke 2017). The reification of a link labeled with the vague catch-all phrase "associated," or reliance on telephone communication patterns alone without reference to other social context, might turn mere delivery boys into nefarious suspects. In a cautionary example from Afghanistan, a special operations unit confused a local political operative with an insurgent pseudonym, and telephone intercepts led them to attack an election convoy (K. Clark 2011). Network diagrams also served a rhetorical role in selling targets to headquarters to approve a direct action. Graphical guilt-by-association made the targeted individual appear more significant in the overall insurgent network.

In principle, the commander's guidance prompts targeting analysts to identify functional "lines of operation" in the insurgent organization (e.g., administration, logistics, propaganda, and combat) and the key operatives who, if removed, might disrupt insurgent operations. In practice, the process worked in reverse. Rather than value-free pictures of the world, SOTF subordinate Task Units seeded their network diagrams around specific

personalities of interest, and then the SOTF headquarters targeting guidance provided a retroactive legitimation of the targets that emerged through idiosyncratic channels. Previous SEAL teams, marine units, intelligence agencies, Iraqi security forces, tribal militias, and Iraqi informants all held opinions about who the "bad guys" in the local area were, and most of them kept target lists and folders on individual suspects. One SEAL mentioned that a target list made a good briefing slide because "it's satisfying to cross bad guys of the list when you get one." Marine battalions unable to get permission from their own chain of command sometimes handed off actionable targets to SOTF Task Units with little advance notice, since the SOTF had a different chain of command. The target pool expanded as working-level analysts or operators took the initiative to follow up leads from a human source, an engagement with local tribal elite, or a signal intercept. The SOTF headquarters held a weekly targeting meeting to gain insight into the targets its three Task Units were pursuing. It maintained a "top-ten" list balanced evenly across them, not because the insurgency was equally active in all areas but rather to avoid the appearance of headquarters favoritism. Headquarters guidance thus did not so much direct targeting, as it organized the ferment of tactical activity into something more coherent and legible for external consumption. It rhetorically demonstrated that the SOTF headquarters was deliberately fighting a war that in fact its Task Units were improvising.

Latour (1987) describes the places where scientists combine inscriptions to gain mastery over distant phenomena as "centers of calculation." The representation closest to something like an apex of incoming and outgoing cascades of inscription in the targeting process was the *PowerPoint* target intelligence package (TIP). The TIP introduced some "nefarious" personage (a word used with surprising frequency), consolidated fusion products about him, and supported construction of the "concept of operations" (CONOP) document operators needed to authorize an assault. TIP slides were usually compiled into "target decks" depicting multiple individuals. Once reified on a TIP, the target *as such* became a black box. The TIP packaged away the equivocation in its creation to present a "bad guy" who should be "actioned."

More machinery was in place for building up a target than for inspecting the quality of construction. Intelligence techs at the lowest echelons faced a great deal of pressure from operators to produce targets. The suppression of skepticism about target quality and disinterest in alternatives to direct action was rarely the result of explicit coercion by operators and more often a matter of self-censorship. By producing targets, moreover, techs could

participate in the "hunt" along with operators, which improved solidarity throughout the military organization. Questioning assumptions or methodologies behind the initial target designation became harder as the hunting process gained momentum, as more collection effort was invested, and as the representational residua of tracking accumulated. The time and effort spent going after a target then reinforced a sense of the target's value.

Data Fragmentation Reinforces Preferences

To access data networks at different levels of classification, personnel relied on several different machines on the same desk. They resorted to thumb drives to move data across them, exposing classified networks that were supposed to be disconnected from unclassified networks to potential infection by malicious viruses or spillage of classified data. Because it was easy to create new digital documents but hard to verify the proper level of classification, most users defaulted to the highest level on their systems, resulting in the routine overclassification of mundane e-mails and *PowerPoint* slides. Other personnel had to make contingent judgments about how to handle or release information at their local level or even to Iraqi partners. Rampant second-guessing undermined the protection that classification controls were supposed to provide.

The SOTF's file server held over a million files, accumulating on average 526 new files per day, half of them duplicates of existing files, dozens duplicated thousands of times, and all saved in a byzantine labyrinth of folders nested ten folders deep on average. These warrens of data were functional for users who lived in them but inscrutable to others spelunking through the share drive. Search engines were nearly useless amid all the duplicate copies, divergent versions, and strange naming conventions. Users thus relied on other users to find things. Electronic mail, the primary means of staff communication, further amplified the clutter by providing users with additional data warrens and more capacity for duplicating data. A new SEAL Team rotated in every six months, and they tended to dump orphaned data into folders with names like "old shit" or "Rob's stuff," and then proceed to rebuild nearly identical content in a new folder. Ubiquitous commercial software, notably Microsoft *Office*, provided the SOTF with considerable "interpretive flexibility" for bottom-up adaptation (Kline and Pinch 1996). Naval Special Warfare culture is generally meritocratic, encouraging operators and techs alike to find unconventional solutions. In principle, users could tailor their local files and then share them across common platforms. Yet with uneven computer expertise at the SOTF, many

ad hoc solutions complicated interoperability. *PowerPoint* became a general-purpose graphics editor and ersatz database for recurrent intelligence and operational reporting "products." *Excel* spreadsheets tracked the recurring flights, missions, targets, logistical tasks, and reports in the routinized military universe. *FalconView*, *Google Earth*, and *ArcGIS* provided geospatial graphics for intelligence data and tactical coordination graphics. Unfortunately, improvisational responses to friction created idiosyncratic material formats that created more friction in other contexts. Users squirreled away important data in the "miscellaneous" fields of structured databases. Detached *PowerPoint* slides proliferated without provenance. *Excel* spreadsheets encoded important data in the visual layout that was not readily legible for automated data processing or statistical analysis without time-consuming human preprocessing.

Digital media did not replace papers and places but rather made them more important (Brown and Duguid 2000; Sellen and Harper 2002). Users leveraged the durability and ergonomics of wall maps, whiteboards, hand-annotated printouts, bureaucratic stamps, mission-support documents, and yellow sticky notes. Paper representations and the local tacit knowledge needed to locate the right digital ones reinforced the importance of physical location. Consequently, physical travel or "battlefield circulation" became necessary for commanders and staff officers to understand the situation at each camp. Remote communications simply advertised the fact that there was even more to learn in person. Action officers sought in-person contact with their counterparts up and down the chain of command in order to orient to and influence one another's behavior.

The SOTF's three Task Units were responsible for twenty different kinds of daily and weekly regular reports as well as endless one-off requests for information from headquarters, which the units usually pushed further down to their Platoons. Forward units that had regular contact with Iraqis constantly received new demands to send additional information, or to repackage the same information in a different format, each requiring production effort and taking time away from the interactions with Iraqis that ostensibly were the subjects of the reports. Each echelon reproduced a fractal variation of the administrative load as they aggregated slides and text for superiors, who each required slightly different formatting and content. "Reach back" entities in the continental United States sought to provide intelligence and other support to forward units, but they also reached forward for dramatic data to advertise their "support to the warfighter" to Beltway audiences. Reach back intelligence tended to specialize in stereotyped tactical support products because, for example, a remote analyst with

no local knowledge could obtain a satellite image of a target building and measure and annotate its dimensions to create a target graphic.

Ironically, the pervasive destabilization of representation had a stabilizing effect on SOTF preferences. Personnel tended to debug systems along well-worn paths supporting direct action rather than use their flexible data systems to refocus on a different aspect of the world. A fragmented organizational operating system labored simply to achieve enough collaboration to enable it to execute the F3EA algorithm *ad infinitum*. The "battle rhythm" of daily, weekly, and monthly briefings, video teleconferences, and reporting focused SOTF personnel on the preparation and coordination of the recurring products required by multiple operational and administrative chains of command. These routine processes both reflected and reinforced the Naval Special Warfare preference for direct action.

Organizing for Direct Action

While the methods for understanding and developing targets were fragmented, organizational processes became better defined and more reliable as target development moved closer to an actual raid. "Pattern of life" analysis accumulated representations of the likely whereabouts of targets with the goal of identifying "triggers" (e.g., activity on a known "selector" associated with a person such as a mobile phone number) that placed a particular individual at a specific location and time frame. Operators took more interest in intelligence at this point because they wanted to improve the reliability and frequency of triggers, which provided more targets to assault. Reliability in this context did not refer to the quality of the target per se, which was an intelligence fusion problem of less interest to operators, but rather that the target (some individual) could be found and overpowered on "the objective" (some location) within some acceptable level of risk to operators. The raid did not so much "service the target" as the targeting process served the raid.

Once the target and objective were reified in the TIP and an actionable trigger was received—all exogenous to mission planning—the logistics of the "full mission profile" followed a well-rehearsed drill. An impromptu planning session with SEAL Platoon leadership determined feasible options for "infiltration," "actions on the objective," and "exfiltration" of the team. Techs scrambled to assemble tactical support products such as maps, imagery, and tactical threat assessments. The Task Unit generated *Word* and *PowerPoint* versions of a standardized CONOP detailing communications, maneuver, and emergency plans. Each CONOP had an information

operations (IO) statement as to the expected effect of the mission and the perceptions that local Iraqis might have of it. This was almost always a vague pro forma statement that the mission would "disrupt the insurgency" and "send a message," with content unspecified. The IO statement varied little from CONOP to CONOP, a testament to the lack of attention given to strategic effectiveness in the political environment versus the tactical performance of direct action.

Task Units tended to wait until the last minute to submit their CONOP, which limited headquarters decision time and made approval more likely. If the SOTF did raise concerns about the low quality of intelligence justifying a target, the Task Unit could counter that direct action would serve as a useful "confidence mission" for training an Iraqi partner force. To check the tendency of SEAL units to indulge in unilateral direct action missions and to encourage more attention to the combat advisory role instead, the SOTF's higher headquarters levied a requirement that there be a minimum two-to-one ratio of Iraqi to American operators on any given mission. The exception to the general reticence at the SOTF to disapprove missions was a concern about "dry holes" (a metaphor expropriated from the petroleum industry to describe an unsuccessful drilling venture), where a raid would fail to find the target on the objective because either he fled or was never there. The SOTF had to negotiate with its headquarters for air support and drone surveillance, which meant taking "high-demand low-density" assets away from other regional SOTFs. Expending these on dry holes made it harder to get them for future missions. Too many false alarms also looked bad on higher-headquarters statistics. The SOTF had a legal officer (judge advocate general [JAG]) who ensured compliance with the laws of war and applicable rules of engagement (ROE; Dunlap 2008). The JAG in the rotation before mine was risk averse and looked for reasons that the commander should disapprove missions. She used ROE to restrain operations and was unpopular with the operators. The JAG in my rotation, by contrast, a reservist who practiced as a corporate lawyer in his civilian life, was risk accepting and looked for ways to approve missions. He used ROE to enable operations and was more popular with the operators. In the final analysis, concerns about excessive operational risk to US personnel, in contrast to concerns about intelligence validity, were most likely to lead to *dis*approval by the SOTF commander.

Once launched, the assault force and the Task Unit coordinated through the common framework structured by the CONOP, shared maps, drone surveillance, Internet chat rooms, and a communication plan with "prowords" (procedure words) keyed to anticipated tactical milestones or

contingencies, often named after athletic teams. Prowords projected on a wall or printed out in the Task Unit operations center enabled the ground commander to efficiently and securely communicate progress along predefined waypoints or branch plans that might require Task Unit action, such as activating a marine quick response force or calling in close air support in the event of enemy contact. "Blue Force Tracking" beacons carried by assaulters in the field broadcast encrypted coordinates to other US units to facilitate coordination in real time. At the same time, the absence of an icon on the common operational picture did not necessarily mean an absence of friendly troops as a beacon could malfunction, the unit could split up, or highly classified missions might preclude public broadcast. Operators drilled these procedures in advance during the eighteen-month predeployment workup, and they helped to orient the Task Unit commander and drone surveillance (ISR) officer supporting the mission.

A larger audience at the SOTF played a more passive role. Headquarters "battle tracking" in practice meant copying *Office* files e-mailed from the Task Unit onto the share drive folder and updating a "mission tracker" spreadsheet as milestones were met. The mission tracker, surprisingly, contained no fields directly linking the mission to target—not even the target's name—and little data concerning mission outcomes. The SOTF's overriding focus was the safe performance of the full mission profile rather than connecting missions to targets and targets to COIN effects. Next to a satellite television displaying either Fox News programs or football games, a projector displayed video from drones (grimly described as "Kill TV") that provided "overwatch" for the assault force, which created a surreal atmosphere of abnormal normalcy. The televised mission enabled deskbound techs to identify vicariously with the heroic operators on the ground. Actual combat was rare during this phase of the war in Anbar, so personnel tended to wander into the TOC out of curiosity and then wander away if there was not much going on.

After mission completion, the Task Unit forwarded a short "blurb" reporting any significant activity on the mission, later followed by a more thorough operations summary and a *PowerPoint* "storyboard." The graphic storyboard, festooned with photographs of any killed or captured Iraqis and weapons material, became the SOTF's trophy of a successful "hunt." If the intended target had been captured, he was labeled a "Jackpot" in large colorful *WordArt* on the *PowerPoint* slide. Any other detainees picked up were simply labeled person under control. The more a mission resonated with commando archetypes, either heroic or tragic, the more detailed and graphic the storyboard. The SOTF e-mailed storyboards out to the wider

Naval Special Warfare community back in the United States, and the most exciting ones formed the core of the team's after action briefs. Performance of the direct action mission translated the *PowerPoint* TIP into the *PowerPoint* storyboard, both of which were readily comprehensible in the Naval Special Warfare worldview.

Attenuated Feedback

In F3EA doctrine, each raid can generate intelligence for the next raid, ultimately leading to the targeting of senior enemy commanders. Evidence collection, document exploitation, forensic analysis, and detainee interrogation are supposed to improve the overall targeting picture by providing more detail on the membership and activities of the enemy organization. The Naval Special Warfare fetish for direct action, however, undermined intelligence processes both before and after the raid. It became more likely that "low-quality" targets (foot soldiers and low-ranking functionaries, who were less likely to know any actionable intelligence) would be nominated, and if the SOTF happened to capture a "high-quality" target (insurgent emirs or lieutenants, who knew something of value), it was less likely that it would "extract" intelligence from the targets.

SEALs treated the exploitation phase of F3EA as more of a cleanup requirement following a successful raid than the set up for follow on raids. Weapons, equipment, documents, pocket litter, cell phones, computers, and other things gathered during a raid could, potentially, have intelligence value for tracking targets as well as evidentiary value for convicting detainees in Iraqi courts. The evidentiary justification of such "sensitive site exploitation" collection usually held more appeal for operators than the intelligence gathering purpose. A guilty prisoner sent to long-term detention justified the risk of a raid and resonated with a heroic narrative, but intelligence analysis was a job for some tech. Intelligence exploitation with a long turnaround time rarely reached the same SEAL team that had recovered the material.

The process of turning detainees into data began with "tactical questioning" on "the objective" (the location of the raid), followed by removal to and interrogation in a detention facility back on base. As SEALs burst into a house, the people inside found themselves facedown on the ground with their hands zip-tied. Fearing for their lives—a natural response to a raid—they were assumed to be more likely to respond to direct questions with veracity than if they had time to compose themselves in captivity. Yet SEALs had to be willing to ask the right questions and care about the

answers. Even if direct questioning provided no information of obvious value, the responses or lack of responses could potentially have enabled operators to triage detainees for expected intelligence utility and to develop approaches for subsequent interrogation. The inclusion of trained interrogators on the assault force, a practice adopted by JSOC, would have improved the effectiveness of the tactical questioning process. However, SOTF "gators" were positioned as lower status "techs" back at camp.

Interrogation uses psychological approaches that, under US military regulations, can only be conducted in controlled detention facilities by certified personnel. Most professionals consider friendlier, seductive approaches to be more effective than fear for eliciting information (Intelligence Science Board 2006; Alexander and Bruning 2008). One unintended consequence of the regulatory controls put in place to prevent prisoner abuse by unskilled interrogators (e.g., at Abu Ghraib) was that skilled interrogators found it harder to build rapport. Intelligence from detainees was subject to the same problems mentioned above of untrustworthy human sources, communication through an interpreter, a bias for targeting intelligence, and the neglect of social and economic detail in reporting (if not in conversation). Yet whereas the SOTF's HUMINT collectors were SEALs who worked, sometimes, outside the wire, the "gators" were techs who worked, always, in prison. Gators had lower status, and when they did not obtain actionable intelligence, SEALs often complained that gators had failed to break their prisoners. They did not like to countenance the possibility that the assaulters had detained an innocent or ignorant Iraqi: "why would we risk our lives to get this guy if he didn't know anything?" The potential innocence of detainees was a sensitive topic for SEALs, for it called into question the judgment of SEAL collectors, Task Unit target development, and the operators who captured the detainees. Interrogation metrics, furthermore, framed success in terms of conviction rates rather than follow-on targeting, thus ignoring the radicalizing effects of incarceration.

The SOTF tended to perform each iteration of the targeting cycle, in sum, as an episodic "one off" rather than a canonical F3EA loop. A process that should have provided useful feedback on the quality of the targeting cycle and new inputs to it became an auxiliary protocol to finish off a direct action mission. Once a Task Unit completed its mission and filed a storyboard, it turned to the next target at the top of its stack, whatever its quality, rather than looking for follow-on targets and patiently analyzing the underground structure of insurgency. There were always more leads available, but the exploitation of prior missions could drag on inconclusively for weeks.

SOTF target development tended to follow independent threads rather than a systematic effort to unravel the fabric of insurgency in Anbar.

Data Friction Inhibits Evaluation

Measured in terms of tactical activity—completed missions, weapon caches discovered, detainees placed in long-term detention, and so on—SOTF operations appeared to be successful. Yet with the ritualized focus on direct action, the strategic effectiveness of the SOTF remained a mystery unto itself. How often did SOTF raids target the names on its target list? Did it capture the people it targeted? Did it retarget when it missed? Did it capture people it did not target? Did detainees provide any useful intelligence about new targets? Did killing and capturing people disrupt the insurgency in Anbar? Were the wrong people harmed? Did indiscriminate raids undermine government legitimacy or exacerbate insurgent recruitment? Was counterterrorism counterproductive for COIN?

If you wanted to answer these questions at the SOTF, you might start by gathering inscriptions generated throughout the F3EA process, referring to the pertinent ontology, such as targets, missions, detainees, and the referents of intelligence reports. You would have to negotiate access with the data owners in each work center or in lateral organizations, understand local coding nuances and sources of friction in each case. Then, you would have to spend time reformatting the data—inconsistent idiosyncrasies across records precluded automation—to make it commensurable across targets and missions and analyze the results. This would take time and effort, and you would need to repeat the process anew to update the results as ongoing operations generated new inscriptions.

The SOTF did not know what it knew, in effect, because data friction made it difficult for personnel to query a fragmented, ersatz, unstructured database to find answers to unanticipated questions. SOTF personnel used their flexible software applications to generate a jumble of ad hoc representational products and processes that supported typical SOTF operations. A channelized information system and the ongoing effort to debug it then guided the SOTF into the repeated performance of one-off raids.

I am *not* claiming that the SOTF deliberately suppressed performance evaluation. Indeed, the US military, to include the Naval Special Warfare community, has a strong technocratic ethos for seeking lessons learned in order to make adjustments in its "tactics, techniques, and procedures" to accomplish the mission as personnel understand it. Encouraged by a pragmatic special operations culture, SOTF personnel constantly tinkered with

data processes, but they often generated negative externalities along the way, that is, incompatible data formats, unreliable data, and security vulnerabilities. They earnestly wanted to do a good job and win the war, however simplistically that objective might have been understood, but working friction made it difficult to appraise their performance, even with respect to organizationally preferred objectives like disrupting the insurgency, to say nothing of less central objectives like economic development or political stabilization. When higher headquarters made inquiries about performance, SOTF officers who lacked the time or ability to understand their own data stores resorted to delegating the work of computing aggregate statistics. They tasked subordinate Task Units with new reporting requirements in specific formats. The frustrations of data friction and the struggles to accommodate it increased endogenously, but always in the direction of established pathways consistent with the commando identity of the organization.

Conclusion

One SEAL officer said to me that the entire Naval Special Warfare community should be put under glass with a sign reading, "break only in case of war." But by late 2007, the political environment in Anbar had transformed into something other than war. Intra-Iraqi politics in Anbar, including tribal vigilantism and initiatives to approach Baghdad for help, together with "nonkinetic" operations by the Marines, had become more important than direct "kinetic" combat. SOTF officers often repeated a COIN mantra, "we can't kill our way out of this," but they were eager to try nonetheless.

In concluding, it is important to highlight my own professional bias in critiquing the bias that the SOTF built into its epistemic infrastructure. I was a reservist tech in charge of indirect action in an organization run by operators trained to conduct direct action. The same position that exposed me to the political complexity of Anbar also distanced me from the ideological center of the SOTF, which remained focused on finding "bad guys." Yet the US disengagement strategy in 2008 was focused on building up the rule of law and transitioning the province to Iraqi control. While JSOC-style counterterrorism *may* have contributed to the temporary improvement in the security situation before mid-2007, afterward the training and engagement missions had become more important for the stabilization of Anbar. The misfortune of the SOTF is *not* that it conducted counterterrorism. Some insurgent operatives were still terrorizing people in the province, and the Euphrates remained a conduit for insurgent logistics supporting the war(s)

still raging in other provinces to the north and east. The tragedy, rather, was that the SOTF reflexively pursued direct action when it had other options; and even then, the inefficiencies in its enabling information work (a form of indirect action) eroded its ability to conduct even direct action efficiently and effectively.

I suspect that the SOTF had little real effect on the viability of AQI. The SOTF performed the F3EA cycle, usually as a series of independent raids rather than a recursive search process, but it was not able to measure its effectiveness. The top targets on its list at the beginning of the deployment were still there at the end. JSOC killed several of them a few years later, but bureaucratic insurgencies like AQI are adept at promoting new commanders, attracting new recruits, and surviving serious attrition (Jordan 2014; Long 2014). Indeed, the institutional core of AQI survived and then reemerged years later as an even more virulent Islamic State (P. B. Johnston et al. 2016). The literature on the strategic effectiveness of targeted killing in general is quite contested (Carvin 2012). Some studies emphasize the economy of force and the abatement of insurgent violence (Byman 2006; Wilner 2010; Strawser 2010; P. B. Johnston 2012; P. B. Johnston and Sarbahi 2016). Others highlight increasing resentment and insurgent recruitment in populations subject to counterterrorism (Cronin 2006; Cavallaro, Sonnenberg, and Knuckey 2012; Boyle 2013; Cronin 2015). At best, targeted killing provides a temporary suppression of insurgency to give nation building efforts a chance to take root. At worst it is actively counterproductive, prolonging the insurgency and the suffering of the civilian population. The risks of targeting errors that kill the wrong people (false positives) have to be balanced against the risks of not engaging active operatives (false negatives). The SOTF, however, was better at controlling tactical errors that immediately affected its own operators rather than either type of intelligence error.

The SOTF was generally better able to reduce friction in the full mission profile because there was a strong institutional consensus about the need to get it right, and there was more salient feedback associated with tactical mission failure (i.e., wounded operators) as opposed to targeting intelligence failure. The persistent friction in the SOTF's data management processes did not cause any spectacular fratricide or obvious civilian casualty incidents during my deployment, but this may have been as much due to good luck as deliberate effort. The real tragedy was that data friction undermined the military effectiveness of both counterterrorism (direct action) and COIN (indirect action). First, the SOTF prioritization of operations over intelligence arguably led it to focus on low level members (who were easier

to find) without disrupting core administrative and logistic elements (which were harder to find) of the insurgent network. Dramatic "Jackpot" storyboards could coexist, in principle, with a thriving underground network that remained illegible. By pursuing several disconnected targets without taking the time to follow up and identify the connections between them, the SOTF could nibble at the edges of the insurgency without affecting its sources of strength (Jones 2009). Second, and more insidiously, raids that disrupted Anbari families and economic relations alienated potential allies and, potentially, aided insurgent recruitment efforts. Individuals are more likely to participate in armed insurgency in response to violations of honor and strong norms of reciprocity in affiliative social networks than through any ideological sympathy with the ostensible political grievances of the insurgency (Petersen 2001; Lindsay and Petersen 2012; Staniland 2014). Targeting errors, therefore, made it more likely that Anbaris would seek vengeance for injured or humiliated kin, support other family members who did so, and withhold support for Coalition initiatives to support the fledgling Iraqi government or join Iraqi security forces. The SOTF's insular epistemic infrastructure controlled tactical risks to operators, while it enabled it to ignore the political ambiguity of Anbar without immediate tactical consequence, even if an angry relative who joined the insurgency might create adverse consequences for future raids.

Much of the recent critical literature on counterterrorism focuses on the use of drones as the "finishing" instrument (Allinson 2015; Chamayou 2015; Cortright, Fairhurst, and Wall 2015; Gusterson 2016). A recurring theme is the mismatch between remote representations and distant social situations that result in tragic civilian deaths. This article has noted some of the ways in which this mismatch can arise (see also Wilke 2017, in this issue). It is important to not overemphasize the novelty of remotely controlled weapons at the expense of the organizations that direct them. Unfortunately, the secrecy of drone operations complicates ethnographic or archival access to the targeting process, not to mention the cultivation of empathy for practitioners (cf. Cullen 2011; McNeal 2014; Mindell 2015). Furthermore, principled disagreement with the policy objectives of counterterrorism is sometimes conflated with concerns about their sociotechnical implementation. If one believes that clandestine targeted killing is categorically wrong, then even a frictionless implementation (whatever that might look like) will be objectionable, and any rationalized process for administering violence will seem inherently distasteful. If, however, one can imagine situations where lethal counterterrorism might be acceptable or even desirable, as in an active combat zone against a determined adversary, then

understanding and controlling the sources and consequences of targeting error becomes an urgent practical matter. For all the outrage against drone strikes, there is perhaps more potential for oversight and professionalism in their conduct than in traditional raiding. Because most of the people who conduct drone strikes are remotely situated (especially when there are no terminal air controllers on the ground as there usually are in close air support scenarios), replicable digital data are necessary for control of most aspects of the process. Therefore, the inscriptions that practitioners produce can more easily be monitored and reviewed by a large network of people within the government. Leaked documents that some critics use as evidence of a sinister killing machine (Scahill 2015) can also be interpreted as evidence of a bureaucracy committed to error checking and accountability (McNeal 2014). Drone operators kill with lawyers and even Presidents looking over their shoulder.

By comparison, the epistemic infrastructure in a tactical special operations unit that picks and prosecutes its own targets in an active combat zone is more problematic. A core institutional problem at the SOTF was the autonomy granted to a tactical organization with strong preferences in an environment where different strategic priorities were more appropriate. Technology did not create this problem, but it did enable and amplify it. Oversight through monitoring and enforcement is the typical solution to this type of agency problem, but the unreliability or inaccessibility of the inscriptions that enable oversight undermine the effectiveness of this remedy. Latour (1987, 227) describes data as "immutable and combinable mobiles" that provide mastery over distant phenomena. Yet in the turbulent particularity of the SOTF, digital slides and spreadsheets were readily copied and altered, not with malign intent to manipulate but in an earnest attempt to accomplish the mission as practitioners understood it—an understanding informed by the organization's commando identity. Data thereby became trapped in idiosyncratic formats on fragmented local networks, and some important knowledge remained trapped in minds that relied on bodies, body armor, and armored vehicles to circulate. Authoritative representations like the target package superficially appeared to be immutable mobiles that provided an authoritative representation of some nefarious personage, which facilitated the approval of a raid. But mutations in their construction and the excision of immobile provenance undermined their referential integrity. By the same token, data about the effectiveness of SOTF raids was difficult to access both within the SOTF and beyond it.

Clausewitz (1976, 88) insists, "The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make

is to establish by that test [of the instrumental purpose of war] the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature." Yet target practice at the SOTF did exactly this. The culture of Naval Special Warfare and many prior years of fierce combat in Anbar primed the organization to seek opportunities for direct action. Pervasive data friction and its proactive accommodation amplified this worldview. The institutionalized practice that identified and reified targets provided the SOTF and its leadership with an impression that direct action was both strategically relevant and tactically possible under the circumstances. The myriad mundane problems that cropped up in the process only helped to underscore both the relevance and the possibility of counterterrorism targeting. This feedback mechanism endogenously amplified the ex ante preferences of the organization, inhibited self-evaluation, and insulated it from countervailing evidence. The strategic situation in Anbar by mid-2007 called for a more political and economic approach to cultivate stability, but the epistemic infrastructure of the SOTF enabled the logic of the hunt to dominate the logic of engagement.

Author's Note

This research leverages my active duty experience in the US Naval Reserve, and this content has undergone classification review by US Naval Special Warfare Command; the results reflect my opinions alone and do not constitute endorsement by the US government.

Acknowledgments

I am very grateful to Lucy Suchman and the editors and anonymous reviewers of this journal for their insightful comments on previous drafts on this article, and to Barry Posen, Wanda Orlikowski, Kenneth Oye, and Merritt Roe Smith for mentorship on the book project from which it is drawn, *Shifting the Fog of War: Information Technology and Human Experience in Military Organizations*. Finally, I thank the men and women of the SOTF for their dedicated service and professionalism in difficult circumstances.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. All emphases in Clausewitz (1976) quotes are in original.
2. SEAL is an acronym for the "sea, air, and land" environments were Naval Special Warfare "frogmen" are trained to operate. Sometimes their reputation could be helpful. During one operation in Anbar, SEALs arrived at a house where the target happened to be watching *Under Siege*, a movie starring Steven Seagal as a disgraced SEAL; the target smiled at encountering the real thing and gave up without a fight.

References

Alexander, Matthew, and John R. Bruning. 2008. *How to Break a Terrorist: The U.S. Interrogators Who Used Brains, Not Brutality, to Take Down the Deadliest Man in Iraq*. New York: Free Press.

Allinson, Jamie. 2015. "The Necropolitics of Drones." *International Political Sociology* 9 (2): 113-27.

al-Jabouri, Najim Abed, and Sterling Jensen. 2010. "The Iraqi and AQI Roles in the Sunni Awakening." *Prism* 2 (1): 3-18.

Ambinder, Marc, and D. B. Brady. 2012. *The Command: Deep Inside the President's Secret Army*. Hoboken, NJ: John Wiley & Sons.

Anderson, Leon. 2006. "Analytic Autoethnography." *Journal of Contemporary Ethnography* 35 (4): 373-95.

Andres, Richard B., Craig Wills, and Thomas E. Griffith. 2006. "Winning with Allies: The Strategic Value of the Afghan Model." *International Security* 30 (3): 124-60.

Bergen, Peter L., and Daniel Rothenberg, Eds. 2014. *Drone Wars: Transforming Conflict, Law, and Policy*. New York: Cambridge University Press.

Beyerchen, Alan. 1992. "Clausewitz, Nonlinearity, and the Unpredictability of War." *International Security* 17 (3): 59-90.

Biddle, Stephen. 2007. "Speed Kills? Reassessing the Role of Speed, Precision, and Situation Awareness in the Fall of Saddam." *Journal of Strategic Studies* 30 (1): 3-46.

Biddle, Stephen, Jeffrey A. Friedman, and Jacob N. Shapiro. 2012. "Testing the Surge: Why Did Violence Decline in Iraq in 2007?" *International Security* 37 (1): 7-40.

Bowker, Geoffrey C., and Susan Leigh Star. 1999. *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: MIT Press.

Boyle, Michael J. 2013. "The Costs and Consequences of Drone Warfare." *International Affairs* 89 (1): 1-29.

Brown, John Seely, and Paul Duguid. 2000. *The Social Life of Information*. Cambridge, MA: Harvard Business Press.

Byman, Daniel. 2006. "Do Targeted Killings Work?" *Foreign Affairs* 85 (2): 95-111.

Carafano, James Jay. 2006. *GI Ingenuity: Improvisation, Technology, and Winning World War II*. Mechanicsburg, PA: Stackpole Books.

Carvin, Stephanie. 2012. "The Trouble with Targeted Killing." *Security Studies* 21 (3): 529-55.

Cavallaro, James, Stephan Sonnenberg, and Sarah Knuckey. 2012. *Living under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan*. New York: International Human Rights and Conflict Resolution Clinic, Stanford Law School and NYU School of Law, Global Justice Clinic.

Chamayou, Grégoire. 2015. *A Theory of the Drone*. Translated by Janet Lloyd. New York: New Press.

Ciborra, Claudio. 2002. *The Labyrinths of Information: Challenging the Wisdom of Systems*. New York: Oxford University Press.

Clark, Andy, and David Chalmers. 1998. "The Extended Mind." *Analysis* 58 (1): 7-19.

Clark, Kate. 2011. *The Takhar Attack: Targeted Killings and the Parallel Worlds of US Intelligence and Afghanistan*. Kabul, Afghanistan: Afghanistan Analysts Network.

Clausewitz, Carl von. 1976. *On War*. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.

Cortright, David, Rachel Fairhurst, and Kristen Wall. 2015. *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*. Chicago, IL: University of Chicago Press.

Cottam, Martha L., Joe W. Huseby, and Bruno Baltodano. 2016. *Confronting Al Qaeda: The Sunni Awakening and American Strategy in Al Anbar*. Lanham, MD: Rowman & Littlefield.

Couch, Dick. 2013. *The Sheriff of Ramadi: Navy Seals and the Winning of Al-Anbar*. Annapolis, MD: Naval Institute Press.

Cronin, Audrey Kurth. 2006. "How Al-Qaida Ends: The Decline and Demise of Terrorist Groups." *International Security* 31 (1): 7-48. doi:10.1162/isec.2006.31.1.7.

Cronin, Audrey Kurth. 2015. "The Strategic Implications of Targeted Drone Strikes for US Global Counterterrorism." In *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications*, edited by David Cortright, Rachel Fairhurst, and Kristen Wall, 99-120. Chicago, IL: University of Chicago Press.

Cullen, Timothy M. 2011. "The MQ-9 Reaper Remotely Piloted Aircraft: Humans and Machines in Action." PhD diss., Massachusetts Institute of Technology, Cambridge.

Der Derian, James. 2009. *Virtuous War: Mapping the Military-industrial-media-entertainment-network*. London, UK: Routledge.

Drew, Christopher. 2010. "Military is Awash in Data from Drones." *New York Times*, January 10, A1.

Dreyfus, Hubert L. 1991. *Being-in-the-world: A Commentary on Heidegger's Being and Time, Division I*. Cambridge, MA: MIT Press.

Dunlap, Charles J. Jr. 2008. "Lawfare Today: A Perspective." *Yale Journal of International Affairs* 3 (1): 146-53.

Eden, Lynn. 2004. *Whole World on Fire: Organizations, Knowledge, and Nuclear Weapons Devastation*. Ithaca, NY: Cornell University Press.

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

Edwards, Paul N. 2010. *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*. Cambridge, MA: MIT Press.

Edwards, Paul N., Matthew S. Mayernik, Archer Batcheller, Geoffrey Bowker, and Christine Borgman. 2011. "Science Friction: Data, Metadata, and Collaboration." *Social Studies of Science* 4 (6): 667-90.

Evangelista, Matthew, and Henry Shue, Eds. 2014. *The American Way of Bombing: Changing Ethical and Legal Norms, from Flying Fortresses to Drones*. Ithaca, NY: Cornell University Press.

Ferris, John. 2004. "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?" *Intelligence and National Security* 19 (2): 199-225.

Ferris, John, and Michael I. Handel. 1995. "Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations." *Intelligence and National Security* 10 (1): 1-58.

Fischhoff, Baruch, and Cherie Chauvin, Eds. 2011. *Intelligence Analysis: Behavioral and Social Scientific Foundations*. Washington, DC: National Academies Press.

Flynn, Michael T., Rich Juergens, and Thomas L. Cantrell. 2008. "Employing ISR: SOF Best Practices." *Joint Forces Quarterly* 50 (3): 56-61.

Forsythe, Diana. 2001. *Studying Those Who Study Us: An Anthropologist in the World of Artificial Intelligence*. Stanford, CA: Stanford University Press.

Galison, Peter. 2010. "Secrecy in Three Acts." *Social Research* 77 (3): 941-74.

Green, Daniel R., and William F. Mullen, III. 2014. *Fallujah Redux: The Anbar Awakening and the Struggle with Al-Qaeda*. Annapolis, MD: Naval Institute Press.

Gusterson, Hugh. 2016. *Drone: Remote Control Warfare*. Cambridge, MA: MIT Press.

Hackett, Edward J. 2005. "Essential Tensions: Identity, Control, and Risk in Research." *Social Studies of Science* 35 (5): 787-826.

Hagan, John, Joshua Kaiser, Anna Hanson, Jon R. Lindsay, Austin G. Long, Stephen Biddle, Jeffrey A. Friedman, and Jacob N. Shapiro. 2013. "Correspondence: Assessing the Synergy Thesis in Iraq." *International Security* 37 (4): 173-98.

Harknett, Richard J. 2000. "The Risks of a Networked Military." *Orbis* 44 (1): 127-43.

Hitz, Frederick P. 2004. *The Great Game: The Myths and Reality of Espionage*. New York: Alfred A. Knopf.

Horowitz, Michael C., Sarah E. Kreps, and Matthew Fuhrmann. 2016. "Separating Fact from Fiction in the Debate over Drone Proliferation." *International Security* 41 (2): 7-42.

Hutchins, Edwin. 1995. *Cognition in the Wild*. Cambridge, MA: MIT Press.

Ihde, Don. 1990. *Technology and the Lifeworld: From Garden to Earth*. Bloomington: Indiana University Press.

Innocenti, Charles W., Ted L. Martens, and Daniel E. Soller. 2009. "Direct Support HUMINT in Operation Iraqi Freedom." *Military Review* 89 (May-June): 48-56.

Intelligence Science Board. 2006. *Educing Information: Interrogation, Science and Art*. Washington, DC: National Defense Intelligence College Press.

Jackson, Colin F. 2008. "Defeat in Victory: Organizational Learning Dysfunction in Counterinsurgency." PhD thesis, Massachusetts Institute of Technology, Cambridge.

Janowitz, Morris. 1959. "Changing Patterns of Organizational Authority: The Military Establishment." *Administrative Science Quarterly* 3 (4): 473-93.

Jasanoff, Sheila S. 1987. "Contested Boundaries in Policy-relevant Science." *Social Studies of Science* 17 (2): 195-230.

Jensen, Sterling. 2014. "Iraqi Narratives of the Anbar Awakening." PhD diss., King's College London, London, UK.

Johnston, Patrick B. 2012. "Does Decapitation Work? Assessing the Effectiveness of Leadership Targeting in Counterinsurgency Campaigns." *International Security* 36 (4): 47-79.

Johnston, Patrick B., and Anoop K. Sarbahi. 2016. "The Impact of US Drone Strikes on Terrorism in Pakistan." *International Studies Quarterly* 60 (2): 203-19.

Johnston, Patrick B., Jacob N. Shapiro, Howard Shatz, Benjamin Bahney, Danielle F. Jung, Patrick Ryan, and Jonathan Wallace. 2016. *Foundations of the Islamic State: Management, Money, and Terror in Iraq, 2005–2010*. Santa Monica, CA: RAND Corporation.

Johnston, Rob. 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study.* Washington, DC: Central Intelligence Agency.

Jones, Derek. 2009. *Understanding the Form, Function, and Logic of Clandestine Cellular Networks: The First Step in Effective Counternetwork Operations*. Fort Leavenworth, KS: School of Advanced Military Studies.

Jordan, Jenna. 2014. "Attacking the Leader, Missing the Mark." *International Security* 38 (4): 7-38.

Kalyvas, Stathis N. 2006. *The Logic of Violence in Civil War*. New York: Cambridge University Press.

Kline, Ronald, and Trevor Pinch. 1996. "Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States." *Technology and Culture* 37 (4): 763-95.

Kollars, Nina. 2014. "Military Innovation's Dialectic: Gun Trucks and Rapid Acquisition." *Security Studies* 23 (4): 787-813.

Lamb, Christopher J., and Evan Munsing. 2011. "Secret Weapon: High-value Target Teams as an Organizational Innovation." Strategic Perspectives No. 4, National Defense University, Center for Strategic Research Institute for National Strategic Studies, Washington, DC.

Latour, Bruno. 1987. *Science in Action: How to Follow Scientists and Engineers through Society*. Cambridge, MA: Harvard University Press.

Latour, Bruno. 1992. "Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts." In *Shaping Technology/Building Society: Studies in Sociotechnical Change*, edited by John Law and Wiebe E. Bijker, 225-58. Cambridge, MA: MIT Press.

Lawson, Sean. 2014. *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age*. New York: Routledge.

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

Lindsay, Jon R. 2013. "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations." *Journal of Strategic Studies* 36 (3): 422-53.

Lindsay, Jon R., and Roger Petersen. 2012. "Varieties of Insurgency and Counterinsurgency in Iraq, 2003-2009." Center for Irregular Warfare and Armed Groups Case Study Series 2011-2012, Naval War College, Newport, RI.

Long, Austin. 2008. "The Anbar Awakening." *Survival* 50 (2): 67-94.

Long, Austin. 2014. "Whack-a-mole or Coup de Grace? Institutionalization and Leadership Targeting in Iraq and Afghanistan." *Security Studies* 23 (3): 471-512.

Long, Austin. 2016. *The Soul of Armies: Counterinsurgency Doctrine and Military Culture in the US and UK. Cornell Studies in Security Affairs*. Ithaca, NY: Cornell University Press.

McCary, John A. 2009. "The Anbar Awakening: An Alliance of Incentives." *The Washington Quarterly* 32 (1): 43-59.

McChrystal, Stanley. 2013. *My Share of the Task: A Memoir*. New York: Penguin.

McMaster, H. R. 2003. "Crack in the Foundation: Defense Transformation and the Underlying Assumption of Dominant Knowledge in Future War." Student Issue Paper, S03-03, US Army War College Center for Strategic Leadership, Carlisle Barracks, PA.

McNeal, Gregory S. 2014. "Targeted Killing and Accountability." *Georgetown Law Journal* 102 (March): 681-794.

McRaven, William H. 1995. *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*. New York: Presidio Press.

Michaels, Jim. 2010. *A Chance in Hell: The Men Who Triumphed over Iraq's Deadliest City and Turned the Tide of War*. New York: Macmillan.

Mindell, David A. 2002. *Between Human and Machine: Feedback, Control, and Computing before Cybernetics*. Baltimore, MD: Johns Hopkins University Press.

Mindell, David A. 2015. *Our Robots, Ourselves: Robotics and the Myths of Autonomy*. New York: Viking.

Montgomery, Gary W., and Timothy S. McWilliams, Eds. 2009. *Al-Anbar Awakening: From Insurgency to Counterinsurgency in Iraq, 2004-2009, Volume II, Iraqi Perspectives*. Quantico, VA: Marine Corps University Press.

Naylor, Sean. 2005. *Not a Good Day to Die: The Untold Story of Operation Anaconda*. New York: Penguin.

Naylor, Sean. 2008. "Petraeus Sounds Off on Afghanistan: General Says Killing or Capturing Bin Laden Not Enough in Battle Against Al-Qaida." *Army Times*, October 21.

Naylor, Sean. 2015. *Relentless Strike: The Secret History of Joint Special Operations Command*. New York: St. Martin's Press.

Noë, Alva. 2009. *Out of Our Heads: Why You Are Not Your Brain, and Other Lessons from the Biology of Consciousness*. New York: Farrar, Straus, and Giroux.

Orlikowski, Wanda J. 2000. "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations." *Organization Science* 11 (4): 404-28.

Oudshoorn, Nelly, and Trevor J. Pinch, Eds. 2003. *How Users Matter: The Co-construction of Users and Technology*. Cambridge, MA: MIT Press.

Owens, William A., and Edward Offley. 2000. *Lifting the Fog of War*. New York: Farrar, Straus and Giroux.

Parker, Ned, and Ali Hamdani. 2006. "How Violence Is Forging a Brutal Divide in Baghdad." *Times of London*, December 14.

Petersen, Roger. 2001. *Resistance and Rebellion: Lessons from Eastern Europe*. New York: Cambridge University Press.

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

Ricks, Thomas E. 2009. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006-2008*. New York: Penguin Press.

Robinson, Linda. 2004. *Masters of Chaos: The Secret History of the Special Forces*. New York: PublicAffairs.

Rosen, Nir. 2009. "An Ugly Peace: What Changed in Iraq." *Boston Review*, December. Availabe at: http://bostonreview.net/archives/BR34.6/rosen.php.

Rothstein, Hy S. 2006. *Afghanistan and the Troubled Future of Unconventional Warfare*. Annapolis, MD: Naval Institute Press.

Russell, James A. 2011. *Innovation, Transformation, and War: Counterinsurgency Operations in Anbar and Ninewa Provinces, Iraq, 2005-2007*. Stanford, CA: Stanford University Press.

Scahill, Jeremy. 2015. "The Assassination Complex: Leaked Military Documents Expose the Inner Workings of Obama's Drone Wars." *The Intercept*, October 15. https://theintercept.com/drone-papers/the-assassination-complex/. Accessed 13 August 2017.

Schultze, Ulrike. 2000. "A Confessional Account of an Ethnography about Knowledge Work." *MIS Quarterly* 24 (1): 3-41.

Searle, Thomas R. 2008. "Tribal Engagement in Anbar Province: The Critical Role of Special Operations Forces." *Joint Forces Quarterly* 50:62-67.

Sellen, Abigail J., and Richard H. R. Harper. 2002. *The Myth of the Paperless Office*. Cambridge, MA: MIT Press.

Shanker, Thom, and Matt Richtel. 2011. "In New Military, Data Overload Can Be Deadly." *New York Times*, January 16, A1.

Shapin, Steven. 1995. "Here and Everywhere: Sociology of Scientific Knowledge." *Annual Review of Sociology* 21:289-321.

Shimko, Keith L. 2010. *The Iraq Wars and America's Military Revolution*. New York: Cambridge University Press.

Shultz, Richard H., Jr. 2013. *The Marines Take Anbar: The Four Year Fight Against Al Qaeda*. Annapolis, MD: Naval Institute Press.

Simons, Anna. 1997. *The Company They Keep: Life Inside the U.S. Army Special Forces*. New York: Free Press.

Smith, Niel, and Sean MacFarland. 2008. "Anbar Awakens: The Tipping Point." *Military Review*, March-April: 41-52.

Snook, Scott A. 2000. *Friendly Fire: The Accidental Shootdown of U.S. Black Hawks over Northern Iraq*. Princeton, NJ: Princeton University Press.

Staniland, Paul. 2014. *Networks of Rebellion: Explaining Insurgent Cohesion and Collapse*. Ithaca, NY: Cornell University Press.

Sterelny, Kim. 2004. "Externalism, Epistemic Artefacts and the Extended Mind." In *The Externalist Challenge: New Studies on Cognition and Intentionality*, edited by Richard Schantz, 239-54. New York: De Gruyter.

Strawser, Bradley Jay. 2010. "Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles." *Journal of Military Ethics* 9 (4): 342-68.

Strawser, Bradley Jay, ed. 2013. *Killing by Remote Control: The Ethics of an Unmanned Military*. New York: Oxford University Press.

Suchman, Lucy A. 2007. *Human-machine Reconfigurations: Plans and Situated Actions*. New York: Cambridge University Press.

Sumida, Jon Tetsuro. 2008. *Decoding Clausewitz: A New Approach to On War*. Lawrence: University Press of Kansas.

Tsing, Anna Lowenhaupt. 2005. *Friction: An Ethnography of Global Connection*. Princeton, NJ: Princeton University Press.

Tucker, David, and Christopher J. Lamb. 2007. *United States Special Operations Forces*. New York: Columbia University Press.

Urban, Mark. 2011. *Task Force Black: The Explosive True Story of the Secret Special Forces War in Iraq*. New York: Macmillan.

U.S. Army. 2006. *FM 3-24: Counterinsurgency.* Washington, DC: Government Printing Office.

U.S. Army. 2015. *FM 3-60: Targeting*. Washington, DC: Government Printing Office.

Van Riper, and Paul K. 1997. *Information Superiority*. Washington, DC: Testimony before U.S. House of Representatives National Security Committee, 20 March.

Vaughan, Diane. 1996. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago, IL: University of Chicago Press.

Virilio, Paul. 1989. *War and Cinema: The Logistics of Perception. Translated by Patrick Camiller.* London, UK: Verso.

Watts, Barry D. 2004. "Clausewitzian Friction and Future War, Revised Edition." McNair Paper, 68, Institute for National Strategic Studies, National Defense University, Washington, DC.

Weick, Karl E. 1995. *Sensemaking in Organizations*. Thousand Oaks, CA: Sage.

Weick, Karl E., and Karlene H. Roberts. 1993. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks." *Administrative Science Quarterly* 38 (3): 357-81.

Wilke, Christiane. 2017. "Seeing and Unmaking Civilians in Afghanistan: Visual Technologies and Contested Professional Visions." *Science, Technology, & Human Values* 42 (6): 1031-60.

Wilner, Alex S. 2010. "Targeted Killings in Afghanistan: Measuring Coercion and Deterrence in Counterterrorism and Counterinsurgency." *Studies in Conflict & Terrorism* 33 (4): 307-29.

Wolters, Timothy S. 2013. *Information at Sea: Shipboard Command and Control in the U.S. Navy, from Mobile Bay to Okinawa*. Baltimore, MD: Johns Hopkins University Press.

Woodward, Bob. 2008. "Why Did Violence Plummet? It Wasn't Just the Surge." *The Washington Post*, September 8.

Author Biography

Jon R. Lindsay is an assistant professor of digital media and global affairs and director of the Trudeau Centre for Peace, Conflict and Justice at the Munk School of Global Affairs at the University of Toronto.