The Promise of Strategic Gain in the Digital Information Age: What Happened?

Dr. Zac Rogers

ABSTRACT

For approximately thirty years an unanswered question has hung over the military enterprise of nation-states: As the digital information age progresses, should we construct a military for the information age, or should we construct an information age military? The former would be an old enterprise applying new tools to its roles and missions. The latter would be a *new enterprise*. The new tools would not only alter the roles and missions the military prosecutes; they would alter the primary purposeful activity of the modern military. The short answer is that militaries and the national security communities that support them have hedged, wary of the uncertainty which comes with complex change. Into this gap has grown a new type of insecurity – a type not confined to military affairs and national security but society-wide – which open societies in particular are yet to fully understand and, thus to develop an appropriate response. The formulation of an appropriate response ties directly back to the thirty-year question. The response, where it exists, is decidedly fragmented. A new addition to the associated lexicon—"cognitive warfare"—has made its way into the discussion and makes no pretense of being confined strictly to military affairs. While a topic of increasing interest, anything resembling a bounded and discrete set of meanings to be associated with cognitive warfare has yet to emerge and seems a way off. This article aims to address this omission and to take stock of how the national security, intelligence, and defense (NSID) communities might begin to approach a coherent understanding of cognitive security. It argues the conflation of operational information warfare with cognitive warfare is a category error that must be addressed first. The hubris of the early digital age provides a lesson to be avoided.

Dr. Zac Rogers, PhD, is Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia. His research combines a traditional grounding in national security, intelligence, and defence with emerging fields of social cybersecurity, digital anthropology, and democratic resilience.

INTRODUCTION

For approximately thirty years an unanswered question has hung over the military enterprise of nation-states: As the digital information age progresses, should we construct a military for the information age, or should we construct an information age military? The former would be an old enterprise applying new tools to its roles and missions. The latter would be a *new enterprise*. The new tools would not only alter the roles and missions the military prosecutes; they would alter the primary purposeful activity of the modern military. The short answer is that militaries and the national security communities that support them have hedged, wary of the uncertainty which comes with complex change. Scholars of war will note that, at least since the Treaty of Westphalia, warfare ultimately has reflected the types of societies which mandate its conduct. However, as John Keegan notes, warrior culture follows society at a distance. In fact, "The distance can never be closed, for the culture of the warrior can never be that of civilisation itself."[1] Into this gap has grown a new type of insecurity, which society at large is yet to fully understand and for which it is yet to mandate an appropriate response. The formulation of an appropriate response ties directly back to the thirty-year question but contains a twist. As the military enterprise has interacted with, incorporated, and in some cases, offloaded capability and responsibility for military-technical innovation to private enterprise, society too is reorienting around those shifts. The roles and statuses of information technologies of control and violence, as a result, are no longer chiefly military business. Yet whose business are they? And how is this changing what we mean by security?

Three overlapping themes, Information Warfare (IW), Dominant Battlespace Knowledge (DBK), and Network-Centric Warfare (NCW), dominated discussion and debate about military-strategic affairs within the

national security, intelligence, and defense (NSID) communities of the United States, its allies, competitors, and adversaries throughout the 1990s. The associated discursive and extra-discursive practices were situated under the rubric of a "Revolution in Military Affairs" and were primarily driven by developments in the application of digital information and communication technologies (ICT) to NSID affairs.[12] Digital ICTs were of course entering every aspect of the civilian domain at the same time, leading to an abundance of scholarship and commentary on the dawning of a networked digital information age or various aspects and iterations of it.[3]

Well into its third decade, the digital age has brought about several variations on these early discussions and the expectations contained therein. In particular, the evolution of IW has, in recent publicly observable episodes, undergone a transformation. Associated in the past primarily with the military battlefield, IW leached into the civilian domain as strategic contests between nation-states in the digital information age became more comprehensive. Today IW is widely understood as endangering the functional viability of entire societies.[4] An explanation as to how this came about has not been forthcoming. The widespread public expectation remains that the NSID community is still in charge and is busy formulating the appropriate and proportionate response to a host of intrusions, influence operations, and outright attacks.

The response, where it exists, is decidedly fragmented, however. A new addition to the associated lexicon—"cognitive warfare"—has made its way into the discussion and makes no pretense of being confined strictly to military affairs. An early criticism of IW was that it seemed to incorporate an indistinct set of themes and boundaries. While a topic of increasing interest, anything resembling a bounded and discrete set of meanings to be associated with cognitive warfare has yet to emerge and seems a way off. This article addresses this omission and then proceeds to take stock of how NSID communities might approach a coherent understanding of cognitive security. It argues the conflation of operational information warfare with cognitive warfare is a category error which must be addressed first. The hubris of the early digital age provides a lesson to be avoided.

From the Information Edge to Cognitive Insecurity

A series of assertions published in *Foreign Affairs* in 1996 by renowned International Relations (IR) scholar Joseph Nye and then U.S. Navy Admiral William Owens captures the prevailing attitude among a good portion of the US NSID community regarding the strategic advantage expected to accrue to the US as the digital information age unfolded:

- Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States.
- (America's) subtle comparative advantage is its ability to collect, process, act upon, and disseminate information, an edge that will almost certainly grow over the next decade.

- This information advantage can help deter or defeat traditional military threats at relatively low cost.
- The information advantage can strengthen the intellectual link between U.S. foreign policy and military power and offer new ways of maintaining leadership in alliances and ad hoc coalitions.
- The United States can use its information resources to engage China, Russia, and other powerful states in security dialogues to prevent them from becoming hostile.[15]

Nye and Owens were expressing what much of the discourse on the digital age of the 1990s had, by the turn of the century, taken as a near-certainty.[6] This cannot be passed off as mere media or academic hype. As Carl Builder noted, it was primarily factions within the US military determined to convince those in and out of uniform who held the purse strings that this was real.[7] Summarily, the prevailing view was that as humanity collectively moved from the industrial age to the information age, from industrial societies to information societies, from industrial warfare to information warfare, and from industrial economies to "knowledge" economies, the investments the US had made in a regime of digital ICTs during the Cold War were set to pay off in spades. The ICT edge was not only militarily relevant—its reach was far broader, and is now even more so.

Like much of post-war defense-led development, digital technology was naively dual-use and would likely magnify advantages as it was incorporated across each sector of society. The profound challenge to organizational structures presented by the digital age would likely also accrue to America's advantage–its open culture and rule of law, entrepreneurial spirit, commitment to market mechanisms, and reification of innovation was not a set of conditions enjoyed by any of its competitors.[8] The digital age would likely multiply US advantage in all these areas, leading to a cascade of advantages shared with allies, with which no rival to US dominance could hope to compete.[9]

If used wisely, the US could leverage its dominance not only to deter open military aggression but to dissuade competitors from even embarking down a path toward direct rivalry.[10] In this way, the US could perhaps become an efficient manager, rather than a costly enforcer, of an increasingly benign post-Cold War international order.[11] While a contentious assertion, the way seemed open, perhaps like never before, for commerce to shade geopolitics as the central theme of strategy and for American society to reap the rewards.[12] If any of this were so, not only the military's roles and missions but its purpose as an enterprise would be under serious review.[13]

The majority of the discourse from this time is rightly careful to point out the possible caveats and potential pitfalls of rushing to a digital future. The wave of enthusiasm, however, was difficult to deny. Barely twenty years on, and in the thick of a now ubiquitously insecure digital age, to reflect on these expectations is to experience a sense of vertigo. Expressing starkly contrasting sentiments, the 2018 US National Defense Strategy states:

> Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.

Of the challenge to American society in the aftermath of Russian interference in the 2016 Presidential election,[14] former U.S. Director of National Intelligence James Clapper writes, "I believe the destiny of the American ideal is at stake."[15] Former NSA and CIA Director General Michael Hayden has described the processes which protect American society from the risk of Hobbesian chaos as being "under stress, and that many of the premises on which we have based our governance, policy, and security are now challenged, eroded, or simply gone."[16]

Scattered throughout the earlier discourse were several salient warnings for digital age enthusiasts. By the late 1990s these warnings increased. Among them, Martin Libicki noted that the quest to "illuminate the battlefield"[17] with a globally situated and connected grid augmented by digital ICTs, which would expedite US and allied networked operations and could make military aggression harder for adversaries to prosecute. This could also be undermined and repurposed as a medium for the propagation of information warfare that leads to a *greater* likelihood of violent confrontation.[18] A monograph produced by RAND Corporation in 1999, while claiming "these changes have affected the global balance of power in favor of the United States," also warned:

> Information that is readily available is available to friend and foe alike; a system that relies on communication can become useless if its ability to communicate is interfered with or destroyed. Because this reliance is so general, attacks on the information infrastructure can have widespread effects, both for the military and for society. And such attacks can come from a variety of sources, some difficult or impossible to identify.[19]

Either an illuminated and therefore less violent battlefield, or an insecure substrate of complex and interconnected vulnerabilities, could be the prevailing outcome of a digital age that cannot be quarantined from the civilian domain. Libicki wrote of the dilemma, "Some systems make it easier for nations to resolve their differences and trust one another; others, by their nature, exacerbate suspicion."[20] Twenty years ago Libicki wrote that the United States had a fundamental choice between these two national defense paths.[21] Builder wrote that the US military found itself torn between a conservative path, of executing existing roles and missions more effectively with the addition of digital ICTs, and a more radical path in which a new type of war and warrior would emerge.[22] Andrew Marshall warned at the same time of the deep uncertainty brought about by the complexity of the coming era.[23] The events of 2016 offer an opportunity to pause and evaluate which path has been taken and its implications.

Information warfare in the national security, intelligence, and defense space is incorporated by a large and multi-disciplinary discourse. Subject areas as diverse as international security and strategic studies, cyber studies, the fourth industrial revolution, and future warfare have all engaged with aspects of IW in often indistinct and overlapping ways.[24] Often the problem with IW is knowing what it is not. Recent events, for example 2016's election interference and 2020's Solarwinds exposure to name just two, have brought renewed attention to the subject, and naturally its concepts and assumptions are evolving as discursive and extra-discursive practices challenge the veracity of existing assumptions about the subject.[25]

Prior to this increased in attention, IW attracted a prolonged wave of consideration from the NSID communities in the United States and those of a host of US partners, competitors, and adversaries in the early 1990s.[26] The focus was concurrent with the increasing application of digital information and communication technologies to NSID affairs and the contemplation of the implications in both IR and Strategic Studies.[27] For militaries, the deluge of data brought on by these new technological inputs engendered a major rethinking about ways, means, and ends with regard to contemporary warfighting, captured by the shift from attrition-based to effects-based operations. Of the thinking behind the shift, Edward Smith, Jr., wrote the following:

> The world in which we live is and always has been complex and filled with ambiguities and uncertainties, and the most complex part of this world has always been man himself – a point that operations in Iraq and Afghanistan underscore every day. Yet, in spite of this pervasive non-linearity, military efforts have tended to focus on linear, attrition-based solutions to linear warfare problems that often have little to do with our messy reality. Effects-Based Operations (EBO) focus on the single most complex aspect of this world: human beings and human organizations.[28]

This shift engendered a mismatch with existing levels of analysis in which tactical, operational, and strategic ends, ways, and means could be usefully demarcated across physical domains for clarity, coordination, and efficiency of effort.[29] The shift from attrition to effects in an unprecedented information-rich environment was to make strategic competition a society-wide, information-centric totality.[30] The traditional strategic art, contending with others for survival on contested terms amid scarcity, would take place in this new materiality. Of EBO, Smith continues:

> They treat national power as a whole and consider its application not just to military operations but across the entire spectrum of competition and conflict from peacetime deterrence, to crisis response, to hostilities in all their varied forms, to the restoration of peace.[31]

Previously well-defined lines of demarcation between military and civilian domains and peace and war were being quietly demolished by forces driven and enabled by the digital age. Publicly available discourse stating this reality among US allies was scarce, perhaps for obvious

reasons, while competitors and adversaries seemed more comfortable making it clear.[32] The digital information age would bring many aspects of strategic competition among nation-states away from the battlefield and more into the civilian domain,[33] and its center of gravity would home in on the mind of the individual–the cognitive agent. As cognitive neuroscientists Moreno and Giordano have noted, the human brain has become the locus of contending in the 21st century.[34] A new term in line with this evolution—"cognitive warfare" (CW)—has recently been used by high-ranking military officials, discussed and debated by military practitioners in formal and informal settings, and is being grappled with by the NSID and academic communities at large.[35] In September 2017, Air Force Chief of Staff, General David L. Goldfein, remarked at the Air, Space, and Cyber Symposium, "We're transitioning from wars of attrition to wars of cognition."[36] At the 2016 DODIIS Worldwide conference, Director of the Defense Intelligence Agency, Lieutenant General Vincent R. Stewart remarked, "How do we win warfare in the information age when the emphasis is as much on the cognitive as much as it is on the kinetic?"[37] The ways in which CW is distinct from IW, if it is distinct, have not been clarified.

Defining the Difference

IW is a battle *for* information where CW is a battle *of* information. Unpacking this simple definition will reveal why this is so, and why CW is a so far under-acknowledged divergence from IW with significant ramifications for the NSID community. Conflating the two is a category error, which stifles understanding, and thus development of the appropriate response. All aspects of operational IW involve actors contending over information within specified and assigned contexts in which the orientation of the context to the contending is settled. CW, conversely, involves actors contending within unspecified and unassigned contexts, in which the orientation of the context literally is the contest. The specification and assignment of context to information is what first gives it meaning, into which a contest can be entered by human actors—it is information which has been de-alienated by a cognitive process. Unspecified and unassigned information exists alienated from context—the contest shifts to the very process of de-alienation in which the information acquires its meaning. It is a cognitive contest and highly asymmetric in favor of the spoiler.

CW is really nothing like "warfare" at all, if we allow for the general heuristic that warfare normally involves contending parties knowingly engaged in the act of contending. Each party understands the context in its own way, but the context represents a minimal shared understanding that a contest has been entered into by the parties concerned. CW to date has been something more akin to terrorism or insurgency, whereby parties are engaged in continuous political opposition punctuated by infrequent acts of public violence against others to cause some often unspecified or frequently amended change in the behavior of the opposing polity. Though these are imperfect analogies. We will need to develop an understanding of a heterogenous type of cognitive violence which can be at once public and deeply private, non-lethal and highly destructive to human intellectual, emotional, and psychological states, blunt and undi-

rected as well as precise and tailored, and most times non-kinetic in the traditional military sense. The type of cognitive violence in mind can easily cause major disruption in the normal functioning of societies as well as significant changes in behavior without being assigned a specified meaning.[38] As Rand Waltzman urged, the time to specify and assign a new cognitive security paradigm is now.[39]

In 1995, Libicki wrote of information warfare, "All forms of struggle over control and dominance of information are considered essentially one struggle, and the techniques of information warfare are seen as aspects of a single discipline."[40] It is difficult to imagine a more all-encompassing description. The official DoD definition did not fare much better on detail. IW was described as:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.[41]

These actions were distinguished in practice by NSID communities into overlapping sub-categories, all involving the protection, manipulation, degradation, and denial of information, and could range from the analog to the digital, be transmitted via anything from carbon to silicon, and could manifest in the oldest forms of conflict to the newest technologies.[42] This taxonomy reflected a unique puzzle regarding information warfare that persists to the present day: if it can be everything at once, what is it not? In what sense and under what terms does it have a beginning and an end? Would battle be joined deliberately or by accident? This enduring puzzle produces another unhelpful problem: if information warfare is essentially indefinable, any definition that does tend to stick will be one imposed on it, often by a single constituency or the most motivated actor. In many ways, this has been the case with IW since the mid-1990s. Alvin Toffler and Heidi Toffler foresaw this predicament in *War and Anti-War* in 1993.[43] Viewing the history of warfare as essentially reflecting the incumbent society's mode of production, the emerging information age would inevitably be the age of an unrestricted and ill-defined new paradigm of information war.

Military organizations most often speak of the struggle for information in the context of the quest for operational situational awareness and in aid of weapon performance. Not particularly advantageous on its own, situational awareness is the foundation of the pursuit of "dominant battlespace knowledge" (DBK).[44] DBK connotes the cognitive capacity required to make effective use of superior situational awareness—to enable and augment the delivery of lethal effects on the battlefield while defending friendly forces from attack. The struggle for information has been understood as involving both offensive and defensive measures, including lines of effort in ISR (Intelligence, surveillance and reconnaissance), EW (electronic warfare), IO (information operations), CyberOps (cyber operations), and PsyOps (psychological operations), conducted to enable the lethal activities common to military organizations.[45] IW in the military domain has

been conducted under the rubric of both conventional and unconventional war involving both regular and irregular forces.[46] These represent specified and assigned modalities of contestation because they are conducted at the operational level.

As Libicki explains, however, while the imperative to conduct lines of IW effort under a unified construct has been acknowledged by US and allied forces since the 1990s, no such unity of effort has emerged despite significant effort, and each line of effort continues to be conducted by separate services in contingent and episodic fashion.[47] Significant advances in each line of effort have been achieved over that time, particularly in the years since 9/11,[48] without the emergence of a coherent and viable framework whereby network effects can leverage the much-desired dominant battle space knowledge. IW efforts have not been unified into a strategic main effort. This is not a failing: it should be understood as a category error that reflects the inherent tension between the two paths noted earlier.

Cognition is at the center of all modes of contending, a foundational assertion in the work of renowned military thinker John Boyd.[49] Boyd's OODA (observe–orient–decide–act) loop is a well known concept within military organizations and beyond, yet arguably its most pivotal element is often overlooked.[50] The core of the OODA loop is the second "O"—orientation. The capacity to observe, decide, and act is meaningless in any form of contending between humans if orientation is left unaddressed. Herein lie the consequences of category error. Orientation is central because any form of contending for information which occurs under conditions of complexity cannot assume the stability of those conditions and therefore the context in which the contending is occurring.

The most fundamental strategic assumption one can make concerns the cognitive conditions in which the contest is occurring—the orientation of the contenders with regard to reality. Arguably Boyd's most fundamental insight, drawing upon and synthesizing a multidisciplinary scientific and philosophical discourse,[51] was that the assumptions of scientific realism, the orientation under which reality is considered a discrete system of objects to which transient human subjects attempt to gain veridical access, is a cognitive weakness and a potentially exploitable vulnerability. Robert Coram summarized the centrality of orientation as follows: "Any inward-oriented and continued effort to improve the match-up of a concept with observed reality will only increase the degree of mismatch."[52] The assumptions of scientific realism applied to complex strategic contending between humans increase the risk of mismatch.[53]

IW, in the way it is conceived and fielded by military organizations, is categorically operational IW. It is in essence a set of inward-oriented and continuous efforts. These efforts have pre-specified and pre-assigned utility and function associated directly or indirectly with supporting the delivery of lethal effects on the battlefield. It is a category error to associate operational IW with the challenge of cognitive security, which has been brought on by the demolishing of boundaries in the digital age. Boyd and others knew that, as information flooded the modern warfighter in the digital age, it would quickly become an impediment if the cognitive

element was not prioritized. DBK is aimed at this goal. However, when strategic contending occurs via unspecified and unassigned modalities which treat the spatial-temporal locus of the contest as everywhere and all the time, as Smith conjectured, DBK does not exhaust the boundaries of the contest. The orientation is the contest. It determines the context and therefore the boundaries of the contest. Operational IW is Popperian science.[54] Cognitive security needs to be Polanyian-Kuhnian science.[55]

The potential of network effects, emerging in parallel with IW and part of the discourse on the digital age (also known as the network age), was also a hugely popular concept from the late 1990s.[56] Proponents of network-centric warfare envisioned an information-rich infrastructure delivering DBK not only to a network of US forces but potentially across allied coalition networks, vastly expanding the capacity to meet future threats to security with a more evenly shared burden of costs and risks.[57] Like IW, NCW struggled to transform from theory to practice. The US has repackaged NCW into its Multi-Domain Operations concept, which is highly derivative of the former.[58] Most contemporary militaries today remain committed to a version of networked warfare, while the scope and scale of early hopes have been dimmed by hard limits on its realization—constraints often more political in nature than technical.[59] Despite some extraordinarily lofty expectations, for the US and allied NSID communities, IW in the digital age is an operational contest for electrons stored in and transiting the electromagnetic spectrum (EMS) via silicon-based infrastructures as adjunct to achieving lethal battlefield effects, the object of the main military effort.

US and allied battlefield experiences in South and Central Asia and the Middle East since 2001 have honed and refined aspects of IW lines of effort, while much of the anticipated strategic level from the domination of digital age warfare is difficult to ascertain. Many would contend it does not exist and has become, in fact, a strategic liability as cognitive insecurity has gripped many of the polities for which the strategic gain was primarily intended.[60] Further iterations of NCW in aid of situational awareness, DBK, and IW, will continue to meet specified and assigned military utility.[61] They will not address the needs of cognitive security. Cognitive security must be assigned a separate category.

Option Dominance?

A review of the discourse on the early military-strategic expectations associated with IW, DBK, and NCW reveals a tale of missed opportunities, if not outright concept failure. That expectations were high is an understatement. According to then Admiral William Owens, writing in 1995, the US could expect to be:

> On the other side of this new revolution in military affairs years, perhaps decades, before any other nation. This is important for many reasons; one of the most significant is that completing the revolution offers us the opportunity to shape the international environment, rather than simply react to it.[62]

All authors writing on these concepts were careful to acknowledge the risks, potential vulnerabilities, and obstacles regarding the pursuit of rapid and highly innovative military transformation. Long lists of technical, political, and organizational challenges were readily admitted. The fundamental view, however, was not readily questioned: the quest to leverage the already extensive US advantage in digital age warfare would lead to outsized strategic gain. The most compelling of these arguments was centered on the concept described by David Alberts as "option dominance".[63] To summarize, option dominance referred to the expectation that, even allowing for the maximum level of push-back across each of the technical, political, and organizational challenge areas, strategic gain would accrue to the US and perhaps a select group of allies and partners.

The source of this relative gain was in the tendency for actors, who might be able to compete and even gain asymmetric advantages in narrow channels of digital age warfare, to be maneuvered nonetheless into a military-technical strategic cul-de-sac by US and allied dominance. Thus, any asymmetric gain would accrue an opportunity cost, which is why Libicki described such methods as second-best.[64] Each opportunity an adversary is forced to forfeit accrues a strategic gain to the dominant actor. The next asymmetric gain forfeits another opportunity cost and so on until the weaker adversary is forced to come to strategic terms in which the dominant military-technical actor holds all the cards. Option dominance was at the heart of NSID community expectations about the military/strategic-level contest likely to play out as the digital age swept through military organizations.[65]

In comments at the beginning of the 1999 RAND monograph, Andrew Marshall delivers what might be the discourse's most overlooked statement: "Information advances will affect more than just how we fight wars. *The nature and purpose of war itself may change.*"[66] The most obvious flaw in the option dominance thesis is that it assumes stability in the context under which the strategic competition is being conducted. An example of inward orientation, it assumes a finite set of options. The assumption of finitude is essential in narrow and discrete contests. It is a liability in open and complex contests. The literature on digital age warfare from the 1990s is more or less unanimous in the implied expectation that its fundamental purpose will be to facilitate application of lethal military force on the physical battlefield. Some allowance for unexpected developments is conveyed, but even the potential for a "black swan" event is understood within the context of the primacy of the lethal contest from which all other political and strategic ends are enabled.

This orientation toward the nature of war has been among the least challenged items in the canon of western military and strategic thought. It atrophies beneath the deep institutional faith in technological supremacy,[67] a well-documented feature of the US orientation toward strategic power (despite Boyd's influence). The costly assumption remains that the most consequential black swan event will be one that emerges in the realm of technology.[68] Unfortunately, the uncertainty about the nature and purpose of strategy to which Marshall was referring

entangles humans with shifting technologies in a complex matrix. A technology-driven black swan has emerged, but under a different orientation. The hyper-connectivity which has accompanied the digital age has exacerbated this condition markedly. As observed by Jeff Reilly, "Advances in technology have subtly nudged the entire globe into a realm where all previous notions of the battle space have been radically altered by domain interdependence."[69]

Cognitive Insecurity is the Hyper-War Offset

The cultivation of "optionality," as expounded by Nassim Nicholas Taleb, is a fundamental strategic necessity in any complex contest.[70] In short, optionality is the ability to discard failure without catastrophic cost while retaining the upside of what is learned. The concept of option dominance has failed because the US and allied NSID communities became unwittingly *obliged to keep* the diminishing strategic returns of the information age. The concept lost its optionality, the ability to *discard* adverse outcomes before they accumulate. The vulnerabilities inherent in the digital substrate highlighted by many early observers have outweighed the benefits, however one might conceive them. The cost of addressing these vulnerabilities grows immense, and what is revealed by recent events is that these costs are not merely technological.

The obligation to keep the adverse effects of the digital age has transformed the contest into one aimed arrow-like at human cognition. Numerous Defense Advanced Research Projects Agency (DARPA) programs search for ways to fill security vulnerabilities in the infrastructures of cyberspace.[71] One study considers whether the US would benefit more than its adversaries if fully homomorphic encryption were developed to the point of widespread use.[72] The authors' findings are highly equivocal about what would be an immensely costly intervention in digital infrastructure. At the same time, the co-evolution of these vulnerabilities with human cognitive vulnerabilities has made it impossible to quarantine people and whole societies from the increasingly sharp strategic contest. DARPA is also the home of a number of programs in which various aspects of the cognitive neurosciences are fully entangled with the strategic contest.[73] Exacerbating this problem is the reliance of the NSID community on the private sector for much of the data gathering and analytics. Marshall acknowledged this in 1999: "The DoD has little control over the pace and direction of the information revolution... (it) needs to manage a difficult transition from being a pioneer to being a leading user."[74]

The psychology and philosophy of cognition, which for centuries was primarily a theoretical question, has become an engineering question. The "cognitive revolution" in psychology, epistemology, and computing beginning in the 1950s[75] has in the past two decades branched into the closely related sciences of "cognitive neuroscience" and "cognitive engineering."[76] Today, these fields sit at the heart of strategic science and technology. DARPA's "Explainable Artificial Intelligence" (XAI) program is indicative of where the fields meet.[77] The race is on to transform advances in machine and deep learning into society-wide strategic assets.[78] For this, the field is endeavoring to make the human-machine interface a zone compatible with normal human tendencies. Machines able to render outputs, no matter how sophisticated, which cannot

mesh with human requirements such as the need for explanation and trust, will not deliver widespread applications.

XAI is aimed at building an "explanation interface" into AI systems, which deliver on this requirement via the inclusion of a causal reasoning module.[79] This need, therefore, to understand and model the "psychology of explanation" is at the heart of the cognitive sciences. For this, the mass data collection and analytics of the Silicon Valley Internet monopolies are invaluable. The relationship between these and other private sector entities and government agencies has been well documented.[80] In the 2017-18 financial year, hundreds of thousands of search warrants, subpoenas, court orders, and other legal requests were put to AT&T, Verizon, and Google by local, state, and federal government authorities in the US.[81] The relationship has its problems.[82] Nonetheless, as it progresses, the full scope of exploitable vulnerabilities in human cognition will be revealed to scientists, and their findings will be available to public and private entities with a myriad of motivations. As Robert McCreight warns:

> If the central goal is to manipulate human thought, emotions, and behaviour through a combination of psychopharmacological, biotechnical, and cybernetic activities and synergized systems to steer, influence, and shape thought and conduct – then we must be and remain alert to such potential goals and progress toward them to date.[83]

No one need posit any nefarious motivations on the behalf of researchers or the NSID community. The simple fact is that each technological epoch society traverses is in part characterized by the ways and means by which humans contend with one another. The human mind has never been fully insulated from this contest. Yet, more and more tools and techniques are becoming available for the exploitation of this space to unprecedented effect, and something of an arms race is accelerating.[84] In addition, the ethics of cognitive neuroscience have been acknowledged as woefully underdeveloped and in urgent need of public attention.[85] The cultivation and exploitation of human attention have become a lucrative enterprise for Silicon Valley monopolists at the same time that its secrets have become of compelling national security interest.[86]

Unfortunately, the confluence of the high economic and strategic value placed on the manipulation of human cognitive processes is having deleterious effects on social stability and the basic functionality of the polity in the US and elsewhere. Warnings from the late 1990s of the inherent uncertainty associated with highly complex information systems have been realized. Numerous challenging questions face the US polity at the same time as the functionality of the polity is frozen and social instability is a rising threat. How should the polity respond to the overwhelming monopoly power of the Silicon Valley giants?[87] What can be done about the widely despised attention-based Internet model that would not crash the value of the NASDAQ?[88] How can foreign interference be thwarted?[89] Does the promise of AI as a military-strategic asset mean the Internet primes are essentially beyond legislative control?[90]

These and many others are the most vexatious questions the US has faced in generations, at the same time its polity is experiencing extraordinary levels of dysfunction. Adversaries and

competitors with even a minimal interest in seeing the US remain dysfunctional, let alone enemies with an interest in system failure, need do little more than seek ways to exacerbate these internal tensions at a chosen time and place.[91] Russia did not need to invent the Internet, the World Wide Web (WWW), portable mobile computing, the attention-based business model, and social media. It has simply used these readily available instruments to cause cognitive chaos, operations which have employed perhaps a hundred operatives.[92] China has used the Internet to acquire troves of intellectual property illegally.[93] The underlying target of both states is the systemic trust which constitutes the sinews of functionality in open democratic societies.[94] This is a prime example of optionality, expertly leveraged.

For their parts, Russia and China have sought to keep features of the digital age useful to them and discard the adverse features. Since 1991, each has pursued a regime of networked and mobile force elements largely aimed at preventing US and allied dominance in the way of war and in strategic competition more generally. Under the anti-access, area denial (A2AD) rubric, the aim is to deny US and allied forces the unimpeded use of the air, sea, land, space, and cyberspace they require to prosecute high-tempo conventional operations.[95] These efforts are asymmetric, as China and Russia have no illusions about meeting US forces at their strongest point. Both have managed to maneuver beneath a line above which a conventional military confrontation with US forces would occur; Russia in the Ukraine and Syria, and China in the South China Sea, are pre-eminent examples. Disruption and denial of the EMS, space elements, and cyberspace are major components of the A2AD approach. US Multi-Domain Operations are geared specifically toward overcoming these challenges. It is, however, in the civilian domain where Russia and China have repurposed the digital age to their strategic advantage and exacerbated the vulnerabilities of US and allied systems.[96]

China is among the world's most connected digital societies, but the Chinese Communist Party (CCP) has pursued a path of tailored social and political control built into the way cyberspace works in China.[97] Its notorious social credit system, which applies the tools of machine learning to mass surveillance, is being tested in multiple provinces.[98] For the most part, it seems Chinese citizens do not harbor major objections to this level of government surveillance, and the CCP's efforts enjoy a level of social and political legitimacy.[99] China has its own indigenous versions of Internet search and social media platforms, through which citizens operate inside a largely invisible firewall, controlled by the CCP, that tailors their online experience.[100]

Russia's digital age is different than China's. Described by Paul and Matthews as a "firehose of falsehoods" model, Russia's approach is to undermine confidence, as broadly as possible, in any information, making the concept of truth contingent and transient.[101] Russia's polity, like all polities, copes with these circumstances in its own culturally and historically contingent way.[102] The ways in which American, Australian, Chinese, Russian, and all cultures are particular in their cognitive proclivities is a topic of great interest. Not covered here, understanding cultural cognitive differences and the foundational assumptions of polities, most importantly

our own assumptions, will be crucial in formulating effective responses to cognitive insecurity. What aspects of our cognitive orientation might be particularly vulnerable to manipulation in the digital age?

Acknowledge and Address the Gap

Militaries draw their mandate and resources exclusively from the state, but we should be mindful that this arrangement is only 372 years old. Human insecurity and conflict are tens of thousands of years old. The digital age has seen the state forfeit a number of its previously held monopolies in short shrift,[103] the consequences of which are only beginning to be felt. The revolution in public-key encryption of the 1970s severed the state's monopoly on privacy and secrecy.[104] Personal computing and the Internet swept away its monopoly on information flow, storage, and security. The capacity to influence has essentially been democratized. Quickly following in tow have been public expectations about the locus and identity of authority and legitimacy, which are fundamental pillars of statehood. Knowledge itself has been under attack for some time.[105] In some parts of the world, the state stands not alone but side-by-side with digital-savvy non-state entities, including criminal gangs, tribal and religious authorities, and corporate actors, in the provision of basic civil services.[106]

The privatization of security services in war zones has risen in the public's consciousness.[107] The financial industry is being disrupted by non-traditional lending and transaction services, and centralized monetary regimes look set for change as cryptographically secured digital currencies emerge to challenge national currencies.[108] There seem to be few enterprises of collective human life not touched by the shifting asymmetries of power enabled by the digital age, and the primary purposeful activities of the associated institutions are adapting. As mentioned in the introduction, the expectation that the NSID community accounts for the locus and source of societal responses to the insecurity of the digital age is widespread. But we have argued that the NSID community, with the military at the forefront, has responsibilities for those activities associated exclusively with operational IW. A category error has obfuscated the growing gap.

The needs of cognitive security in the digital age are of a different type. The digital age has changed society and the military, but the most important factor is how it has changed the relationship between the two. The question put by Builder in 1999 was to what extent the digital age would alter the primary purposeful activity of the military, its "enterprise."[109] Would it simply seek to apply new tools to an old enterprise, or would the new tools fundamentally change the enterprise, as was the case with mechanized war, nuclear weapons, and the opening of space in the 20th century? These changes took time to mature, and any answer to Builder's question remains pending. What seems undeniable is that the military enterprise in the digital age has changed significantly and unpredictably, and that these changes are in their infancy. The transformation continues, and the gap between the demand for and the supply of security products and services has widened while we await their maturation.

The NSID community is entangled in a complex and difficult transformation brought on by the digital age. Multiple and conflicting imperatives and motivations are in play, but the public sees only fragments of these tensions in debates over privacy and secrecy, surveillance and security, monopoly and democracy, and so on. Cognitive insecurity of the sort that has destabilized and disrupted American society since the 2016 election is a manifestation of the unpredictable nature of complexity, complexity both exacerbated so acutely by hyper-connectivity and turned into a quasi-extractive industry by Silicon Valley.[110] A growing number of experts are forwarding a view, however, that the needs of cognitive security for open societies in the digital age cannot be met by military enterprise alone.[111] In 1999, Builder presaged a greater burden for civil society:

> Defensive information warfare may turn out to be the distributed burden of society every bit as much as its military—where all who use the fruits of the information revolution, civilian or military, must look after their own protection.[112]

Clint Watts, a former FBI Special Agent who has worked for years countering radical extremism inside and outside official channels,[113] believes slow-to-adapt government institutions are not the answer when it comes to contending with digital information operations. Watts has advocated for the growth of online civilian armies of digital defenders—cyber-educated guerrillas able to detect, deny, and disrupt enemy incursions into the cognitive battle space.[114] In truth, a model of amateur online warriors, receiving implicit and deniable approval from government agencies, is one exploited by Russian and Chinese authorities for some time. Rand Waltzman, who created DARPA's Social Media in Strategic Communication program,[115] believes "the nature of interactions with the information environment are rapidly evolving and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defences."[116] Waltzman advocates bringing together: "Cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology to develop a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues."[117]

Cognitive security is a unique challenge in that it traverses the security architecture of open societies, between policing criminal activity and countering the activities of malicious foreign agents. The reality is that these domains are unified at the digital machine/human interface, and so must be the response,[118] but the response is not merely a technological one. The institutional role of the military in the social fabric of open society has always extended beyond the battlefield. As a trusted social institution, and a resource of great depth, history, and stability, its role in pushing its values forward as the institutional life of open society is changing should not be overlooked.[119] We build trust side-by-side and bottom-up. Only by doing so can the fruits of the digital age be retained, and its dangers, flaws, and errors mitigated. Strategic gain in the digital age will depend on building this trust.

CONCLUSION

A good deal of skeptical caution should also be applied. The hubris which convinced many that the digital information age would supply a strategic *fait accompli* to US and allied competitors has been met sharply by unpredictable reality. In the same way, beliefs that advances in deep-learning AI and other data-driven tools and methods can be applied to the society-centric contest, to gain strategic advantage over the adversaries of open democratic societies, rely on dangerous assumptions.[120] For proponents of narrative warfare, the questions of narrative fratricide, blowback, and the unanticipated side effects of their interventions loom large. Can and should open democratic societies seek to manipulate the manipulators? Game the gamers? What are the implications of these measures, which are certain to create even more mass distrust, for the fabric of trust on which open society depends?[121] As Josh Kerbel puts it, could calls for states to engage in narrative warfare be an example of "activity masquerading as progress"?[122] What of the unintended consequences of that activity? Society-centric war is an attack on the sinews of trust that bind and facilitate open societies, enabled nowadays by the digital medium. Responses that risk the further erosion of the social fabric by gamifying societal functionality via the digital medium swallow that bait. The strategic task is great and requires a whole-of-society response: How to live freely and securely in the technological landscapes we have created, deployed, and scaled, and whose wisdom we now question.

NOTES

1. John Keegan, *A History Of Warfare* (Random House, 2011), xvi.
2. For excellent review of this discourse see Sean T. Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Routledge, 2013); Sean Lawson, "Cold War Military Systems Science and the Emergence of a Nonlinear View of War in the US Military," *Cold War History* 11, no. 3 (August 1, 2011): 421-40, https://doi.org/10.1080/14682745.2010.494302.
3. For canonical overview see Manuel Castells, *The Information Age, Volumes 1-3: Economy, Society and Culture* (Wiley, 1999); Manuel Castells, "Materials for an Exploratory Theory of the Network Society," T*he British Journal of Sociology* 51, no. 1 (2000): 5-24.
4. Maryanne Kelton et al., "Australia, the Utility of Force and the Society-Centric Battlespace," *International Affairs,* May 28, 2019, https://doi.org/10.1093/ia/iiz080.
5. Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs,* 1996, 20-36.
6. Notable exceptions included Barry D. Watts, *Clausewitzian Friction and Future War* (DIANE Publishing, 1996); Charles J. Dunlap, Jr., "21st-Century Land Warfare: Four Dangerous Myths," *Parameters,* Autumn 1997, https://ssi.armywarcollege.edu/pubs/Parameters/articles/97autumn/dunlap.htm.
7. Zalmay Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare* (RAND Corporation, 1999), 22, http://www.rand.org/pubs/monograph_reports/MR1016.html.
8. Edward Luttwak, *Turbo-Capitalism: Winners and Losers in the Global Economy (*New York: HarperCollins Publishers, 1999).
9. Patrick E. Tyler, "U.S. Strategy Plan Calls for Ensuring No Rivals Develop," *The New York Times,* March 8, 1992, sec. World, http://www.nytimes.com/1992/03/08/world/us-strategy-plan-calls-for-insuring-no-rivals-develop.html.
10. Richard L. Kugler, "Dissuasion as a Strategic Concept" (Fort McNair, Washington, DC: National Defense University Institute for National Strategic Studies, 2002), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA421905.
11. G. John Ikenberry, *America Unrivaled: The Future of the Balance of Power* (Cornell University Press, 2002).
12. Edward N. Luttwak, "From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce," The National Interest, no. 20 (1990): 17-23; Richard Nixon, *Seize the Moment: America's Challenge in a One-Superpower World* (Simon and Schuster, 2013).
13. The September/October edition of *Foreign Affairs* is noteworthy on this topic, https://www.foreignaffairs.com/search?qs=september+october+1997.
14. US Intelligence Community, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution" (Office of the Director of National Intelligence, January 6, 2017), https://publicintelligence.net/odni-russian-election-operations/; Senate Select Committee on Intelligence, "The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections" (United States Senate, July 3, 2018), https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.
15. James R. Clapper and Trey Brown, *Facts and Fears: Hard Truths from a Life in Intelligence* (Penguin, 2018).
16. Michael V. Hayden, *The Assault on Intelligence: American National Security in an Age of Lies (*Penguin, 2018).
17. Martin C. Libicki, *Illuminating Tomorrow's War* (DIANE Publishing, 1999).
18. Martin C. Libicki, "Information War, Information Peace," *Journal of International Affairs* 51, no. 2 (1998): 411.
19. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* iii.
20. Libicki, 411-12.
21. Libicki, 411.
22. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 21.
23. Khalilzad et al., 1-6.

NOTES

24. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge University Press, 2007); Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5 (2011), http://elastic.org/~fche/mirrors/www.cryptome.org/2013/07/cyber-war-racket-0012.pdf; John B. Sheldon, "Deciphering Cyberpower Strategic Purpose in Peace and War," *Strategic Studies Quarterly: SSQ; Maxwell Air Force Base* 5, no. 2 (Summer 2011): 95-112; John Arquilla, "Can Information Warfare Ever Be Just?" *Ethics and Information Technology; Dordrecht* 1, no. 3 (1999): 203-12; Dorothy Elizabeth Robling Denning, *Information Warfare and Security* (ACM Press, 1999); Roger C. Molander et al., *Strategic Information Warfare: A New Face of War* (Rand Corporation, 1996); Klaus Schwab, *The Fourth Industrial Revolution* (New York: Crown Business, 2017); Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Warner Books, 1994); Carmine Cicalese, "Redefining Information Operations," *Joint Force Quarterly/ National Defense University* 69 (April 2013); Frans P.B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2007); D. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Springer, 2015); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015); Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades," in *The Global Politics of Science and Technology - Vol. 1,* Global Power Shift (Springer, Berlin, Heidelberg, 2014), 91-113, https://doi.org/10.1007/978-3-642-55007-2_5.
25. Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," *The Asan Forum* (blog), May 8, 2018, http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/; Thomas Mahnken, Ross Babbage, and Toshi Yoshihara, "Countering Comprehensive Coercion: Competitive Strategies Against Authoritarian Political Warfare" (Center for Strategic and Budgetary Assessments, May 2018), https://csbaonline.org/uploads/documents/Countering_Comprehensive_Coercion%2C_May_2018.pdf; James Scott and Drew Spaniel, *China's Espionage Dynasty: Economic Death by a Thousand Cuts* (CreateSpace Independent Publishing Platform, 2016); Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg* (blog), October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2; James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in *Cyber War in Perspective: Russian Aggression Against Ukraine* (Tallinn: NATO CCD COE Publications, 2015); Senate Select Committee on Intelligence, "The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections"; Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model" (Santa Monica, California: RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.
26. John Arquilla, "The Strategic Implications of Information Dominance" (Calhoun Institutional Archive of the Naval Postgraduate School, 1994); Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Spring 2017, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-1/Libicki.pdf; H.R. McMaster, "Crack in the Foundation: Defense Transformation and Underlying Assumption of Dominant Knowledge in Future War," *Center for Strategic Leadership, U.S. Army War College* S03, no. 3 (November 2003), http://www.au.af.mil/au/awc/awcgate/army-usawc/mcmaster_foundation.pdf; Alicia Wanless and Michael Berk, "The Strategic Communication Ricochet: Planning Ahead for Greater Resiliency," *The Strategy Bridge* (blog), March 7, 2018, https://thestrategybridge-org.cdn.ampproject.org/c/s/thestrategybridge.org/the-bridge/2018/3/7/the-strategic-communication-ricochet-planning-ahead-for-greater-resiliency?format=amp; David S. Alberts et al., *Understanding Information Age Warfare*, n.d.; Emily Goldman and Thomas G. Mahnken, *The Information Revolution in Military Affairs in Asia* (Palgrave Macmillan, 2004); Peter Hall and Robert Wylie, "The Revolution in Military Affairs and Australia's Defense Industry Base, 1996-2006," *Security Challenges Volume 4, Number 4 (Summer 2008), 57-80*, accessed February 2, 2015, http://www.securitychallenges.org.au/ArticlePages/vol4no4HallandWylie.html; Wang Xiangsui and Qiao Liang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999); Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review*, February 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.
27. Arquilla, "The Strategic Implications of Information Dominance"; John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1, 1993): 141-65, https://doi.org/10.1080/01495939308402915; John Arquilla et al., *The Emergence of Noopolitik: Toward An American Information Strategy* (Rand Corporation, 1999); Martin Libicki, "The Emerging Primacy of Information," *Orbis* 40, no. 2 (1996): 261-274.
28. Edward A. Smith, Jr., "Effects-Based Operations," *Security Challenges* 2, no. 1 (2006): 43, https://www.regionalsecurity.org.au/Resources/Files/vol2no1Smith.pdf.

NOTES

29. Edward A. Smith, Jr., *Effects Based Operations: Applying Network Centric Warfare to Peace, Crisis, and War* (DOD-CCRP, 2002).
30. Ariel E. Levite and Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-Centric Warfare," *Survival* 60, no. 6 (November 2, 2018): 91-118, https://doi.org/10.1080/00396338.2018.1542806.
31. Smith Jr., "Effects-Based Operations," 43.
32. Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice*, 1st edition (Foreign Military Studies Office, 2004), https://babel.hathitrust.org/cgi/pt?id=uiug.30112065967041;view=1up;seq=37; Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy"; Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin* (Brookings Institution Press, 2015); Peter Pomerantsev, "The Hidden Author of Putinism," *The Atlantic*, November 7, 2014, https://www.theatlantic.com/international/archive/2014/11/hidden-author-putinism-russia-vladislav-surkov/382489/; Scott and Spaniel, *China's Espionage Dynasty*.
33. Emile Simpson, *War From the Ground Up: Twenty-First Century Combat as Politics* (Oxford University Press, 2012); Richard D'Aveni, "Waking Up to the New Era of Hypercompetition," *Washington Quarterly* 21 (March 1, 1998): 183–95, https://doi.org/10.1080/01636609809550302.
34. Jonathan D. Moreno, *Mind Wars: Brain Science and the Military in the Twenty-First Century* (Bellevue Literary Press, 2012); James Giordano, ed., *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Press, 2014).
35. General David L. Goldfein, "Air Force Association Remarks" (September 19, 2017), http://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf; Vincent R. Stewart, DoDIIS Worldwide Conference Opening Remarks (Atlanta, Georgia, 2017), https://vimeo.com/206476865; *Exploring Cognitive Warfare*, Over the Horizon, n.d., https://othjournal.com/2017/11/08/oth-podcast-4-exploring-cognitive-warfare/; Tyler Quinn and Von Lambert, "Musings on the Prominence of Informational Effects in the Operational Art," Grounded Curiosity, May 21, 2018, https://groundedcuriosity.com/musings-on-the-prominence-of-informational-effects-in-the-operational-art/; John Michael Fabry, "Information Warfare: Expanding the Paradigm" (Ph.D., Rutgers The State University of New Jersey - New Brunswick, 1998), https://search.proquest.com/docview/304453551/abstract/1D00BD1F4AA1468FPQ/1; Rand Waltzman, "A Center for Cognitive Security - Draft Proposal," *IPA Information Professionals Association.* (blog), April 18, 2017, https://information-professionals.org/a-center-for-cognitive-security-draft-proposal/; Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," SIGNAL Magazine, August 15, 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle; Emily Bienvenue, Zac Rogers, and Sian Troath, "Cognitive Warfare: The Fight We've Got," The Cove, September 19, 2018, https://www.cove.org.au/adaptation/article-cognitive-warfare-the-fight-weve-got/; George Popp, Sarah Canna, and N. Peterson, eds., "From Control to Influence? A View of – and Vision for – the Future" (10th Annual Multilayer Assessment (SMA) Conference, Joint Base Andrews, 2017), http://nsiteam.com/social/wp-content/uploads/2017/06/U_Final_SMA-Conference-Proceedings-25-26-April-2017.pdf; Rand Waltzman, "The Weaponization of Information: The Need for Cognitive Security," § Senate Armed Services Committee, Subcommittee on Cybersecurity (2017), https://www.rand.org/pubs/testimonies/CT473.html.
36. Goldfein, "Air Force Association Remarks."
37. Stewart, DoDIIS Worldwide Conference Opening Remarks.
38. Lauren Elkins, "The 6th Warfighting Domain," OTH, November 5, 2019, https://othjournal.com/2019/11/05/the-6th-warfighting-domain/.
39. Waltzman, "A Center for Cognitive Security – Draft Proposal"; Waltzman, The Weaponization of Information: The Need for Cognitive Security.
40. "Martin C. Libicki, "What Is Information Warfare?" (National Defense University: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, August 1995), x, http://www.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf.
41. Office of the Chairman of the Joint Chiefs of Staff, "Joint Information Warfare Policy" (Washington, DC: Chairman of the Joint Chiefs of Staff Instruction 3210.01, January 2, 1996).
42. Libicki, "What Is Information Warfare?" x.
43. Toffler and Toffler, *War and Anti-War.*

NOTES

44. David S. Alberts, "The Future of Command and Control with DBK," in *Dominant Battlespace Knowledge* (National Defense University, 1995); Paul Bracken, "The Significance of DBK," in *Dominant Battlespace Knowledge* (National Defense University, 1995); Martin Libicki, "DBK and Its Consequences," in *Dominant Battlespace Knowledge* (National Defense University, 1995), http://www.dodccrp.org/files/Libicki_Dominant.pdf.
45. Libicki, "The Convergence of Information Warfare."
46. U.S. Army, "Army Special Operations Forces Unconventional Warfare," September 30, 2008, https://file.wikileaks.org/file/us-fm3-05-130.pdf; U.S. Marine Corps Combat Development Command and U.S. Special Operations Command Center for Knowledge and Futures, "Multi-Service Concept for Irregular Warfare," August 2006, https://file.wikileaks.org/file/us-iw-multi-service-2006.pdf; John Strand, *Offensive Countermeasures: The Art of Active Defense*, 2nd ed. (John Strand Paul Asadoorian, 2017); Wyatt Hoffman and Ariel E. Levite, "Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?" (Carnegie Endowment for International Peace, June 14, 2017), http://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236; James Lewis, "Rethinking Cybersecurity: Strategy, Mass Effects, and States," CSIS Technology Program (CSIS, January 2018).
47. Libicki, "The Convergence of Information Warfare."
48. Robert Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), 17.
49. See biographies of Boyd's life and work, Osinga, *Science, Strategy and War*; Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (Hachette UK, 2002); and Boyd's unpublished work accessible at John R. Boyd, "Patterns of Conflict," *A Discourse on Winning and Losing, (unpublished manuscript)*, 1987, http://dnipogo.org/john-r-boyd/; John R. Boyd, "Destruction and Creation," *A Discourse on Winning and Losing, (Unpublished Manuscript)*, 1987, http://dnipogo.org/john-r-boyd/.
50. Ian Brown, "Opening the Loop: A Look inside the Mind of John Boyd," *Marine Corps Gazette*, June 2015, https://www.mcafdn.org/gazette/2015/06/opening-loop.
51. Osinga, *Science, Strategy and War,* chaps. 4-5.
52. Coram, *Boyd*, 120.
53. Explored most prominently over three decades in the work of Donald D. Hoffman, *The Case Against Reality: How Evolution Hid the Truth from Our Eyes* (Penguin UK, 2019).
54. Popper introduced the assertion that scientific knowledge can only progress through falsification. Unspecified and unassigned items of knowledge about the world are by definition unfalsifiable and do not count as knowledge under this formulation. Operational IW is Popperian in the sense that it involves making discrete claims about narrow aspects of the world which are falsifiable. Karl Popper, *The Logic of Scientific Discovery* (Routledge, 2005); Karl Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge* (Routledge, 2014).
55. Polanyi and Kuhn offer responses to Popper which support the view that falsifiable claims alone cannot account for the growth of knowledge. Michael Polanyi, *The Tacit Dimension* (University of Chicago Press, 2009); Thomas S. Kuhn, *The Structure of Scientific Revolutions: 50th Anniversary Edition* (University of Chicago Press, 2012).
56. Manuel Castells, *The Information Age*, Volumes 1-3: Economy, *Society and Culture* (Wiley, 1999); Joshua Cooper Ramo, *The Seventh Sense: Power, Fortune, and Survival in the Age of Networks* (New York: Little, Brown and Company, 2016); David S. Alberts, John J. Garstka, and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd ed. (DoD C4ISR Cooperative Research Program, 2000).
57. Paul T. Mitchell, *Network Centric Warfare and Coalition Operations: The New Military Operating System* (Routledge, 2009); Martin C. Libicki, *Illuminating Tomorrow's War* (DIANE Publishing, 1999); Martin C. Libicki and Stuart E. Johnson, eds., "Dominant Battlespace Knowledge" (National Defense University, October 1995), http://www.dodccrp.org/files/Libicki_Dominant.pdf.
58. Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air & Space Power Journal* 30, no. 1 (2016): 61; Maj Sean A. Atkins, USAF, "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace," *Air & Space Power Journal,* Fall 2018, https://www.airuniversity.af.mil/ASPJ/; Albert Palazzo, "Multi-Domain Battle: The Echo of the Past," *The Strategy Bridge* (blog), October 11, 2017, https://thestrategybridge.org/the-bridge/2017/10/11/multi-domain-battle-the-echo-of-the-past.

NOTES

59. C. Kopp, "Fifteen Constraints on the Capability of High-Capacity Mobile Military Networked Systems," July 2007, http://search.informit.com.au/documentSummary;dn=090370892216290;res=IELENG; Paul T. Mitchell, "Freedom and Control: Networks in Military Environments," *The Adelphi Papers* 46, no. 385 (December 1, 2006): 27-44; Stanley A. McChrystal, "It Takes a Network," *Foreign Policy* (blog), accessed November 16, 2015, https://foreignpolicy.com/2011/02/21/it-takes-a-network/; Gary A. Whitted and Captain Mary E. Just, "Advanced Collaborative Technologies Supporting the 21st Century Warfighter in a Network Centric Environment" (Proceedings of the 2005 International Symposium on Collaborative Technologies and Systems, IEEE Conference Publications, May 2005).
60. Nate Freier et al., "Game On or Game Over: Hypercompetition and Military Advantage," US Army War College War Room, May 22, 2018, https://warroom.armywarcollege.edu/articles/the-new-defense-normal-nine-fundamentals-of-hypercompetition/; Mari Eder, "The Information Apocalypse… Is Already Here," US Army War College War Room, August 22, 2018, https://warroom.armywarcollege.edu/articles/information-apocalypse/; Hezekiah Winter, "Total Disinformation Warfare," Hacker Noon, June 9, 2018, https://hackernoon.com/on-russian-and-washington-propaganda-c95f553a6776.
61. Peter Layton, "Fifth Generation Warfare: An Evolving Technical Dimension of War," Over the Horizon, July 31, 2017, https://overthehorizonmdos.com/2017/07/31/5th-gen-warfare/; Peter Layton, *Algorithmic Warfare Applying Artificial Intelligence to Warfighting* (Air Power Development Centre, 2018), http://airpower.airforce.gov.au/APDC/media/PDF-Files/Contemporary%20AirPower/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf; Peter Layton, "America's Air Power Revolution," *Defense Today*, March 2018, https://drive.google.com/file/d/1On7yP-dPtGx4f4dDVb2g5G5zxv2OkeZNL/view.
62. Libicki and Johnson, "Dominant Battlespace Knowledge," v.
63. Libicki and Johnson, 33.
64. Libicki and Johnson, 19.
65. Arquilla et al., *The Emergence of Noopolitik*; Arquilla, "The Strategic Implications of Information Dominance."
66. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare*, 1, emphasis added.
67. Col. Michael W. Pietrucha, "The Search for the Technological Silver Bullet To Win Wars," War on the Rocks, accessed September 2, 2015, http://warontherocks.com/2015/08/the-search-for-the-technological-silver-bullet-to-win-wars/.
68. Christian Davenport, "Efforts Underway to Improve Pentagon's Procurement System," *The Washington Post*, December 1, 2014, https://www.washingtonpost.com/business/economy/why-the-pentagon-spent-46b-on-12-weapon-programs-it-never-finished/2014/12/01/c1787814-74f7-11e4-9d9b-86d397daad27_story.html; Mike Pietrucha, "The Phantom Menace: When Threat Capabilities Are Made Up," War on the Rocks, September 21, 2016, http://warontherocks.com/2016/09/the-phantom-menace-when-threat-capabilities-are-made-up/.
69. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," 67.
70. Nassim Nicholas Taleb, *Incerto: Antifragile, the Black Swan, Fooled by Randomness, the Bed of Procrustes* (Random House Publishing Group, 2016).
71. Brad D. Williams, "DARPA Moves to Innovate Cyber Intel Capability with Real-Time Threat Visualization," Fifth Domain | Cyber, June 23, 2017, http://fifthdomain.com/2017/06/23/darpa-moves-to-innovate-cyber-intel-capability-with-real-time-threat-visualization/; DARPA, "DARPA Seeks More Robust Military Wireless Networks," DARPA, March 18, 2013, https://www.darpa.mil/news-events/2013-03-18; Nicole Blake Johnson, "DARPA's Cyber Antidote," *FedTech*, June 3, 2014, https://fedtechmagazine.com/article/2014/06/darpas-cyber-antidote; John Launchbury, "PROgramming Computation on EncryptEd Data (PROCEED)," DARPA, accessed April 10, 2017, http://www.darpa.mil/program/programming-computation-on-encrypted-data; Martin C. Libicki et al., "Ramifications of DARPA's Programming Computation on Encrypted Data Program" (National Defense Research Institute: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR567/RAND_RR567.pdf.
72. Libicki et al., "Ramifications of DARPA's Programming Computation on Encrypted Data Program."
73. Jonathan D. Moreno, "DARPA on Your Mind," Cerebrum, October 1, 2004, http://www.dana.org/Cerebrum/Default.aspx?id=39170; Joshua Elliot, "Active Social Engineering Defense (ASED)," DARPA, n.d., https://www.darpa.mil/program/active-social-engineering-defense; Justin Sanchez, "Narrative Networks," DARPA, n.d., https://www.darpa.mil/program/narrative-networks; DARPA, "Social Media in Strategic Communication (SMISC)," DARPA, n.d., https://www.darpa.mil/program/social-media-in-strategic-communication; DARPA, "Social Systems," DARPA, n.d., https://www.darpa.mil/about-us/dso-social-systems; Matthew Hepburn, "Strategic Social Interaction Modules (SSIM)," DARPA, n.d., https://www.darpa.mil/program/strategic-social-interaction-modules; Justin Sanchez, "Systems-Based Neurotechnology for Emerging Therapies (SUBNETS)," DARPA, n.d., https://www.darpa.mil/program/systems-based-neurotechnology-for-emerging-therapies.

NOTES

74. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 2.
75. Howard E. Gardner, *The Mind's New Science: A History Of The Cognitive Revolution* (Hachette UK, 2008); Norbert Wiener, *The Human Use Of Human Beings: Cybernetics And Society* (Hachette UK, 1988); Gilbert Ryle, *The Concept of Mind: 60th Anniversary Edition* (Routledge, 2009); Gregory Bateson, *Mind and Nature: A Necessary Unity* (Hampton Press, 2002).
76. John T. Wixted and John Serences, eds., *Stevens' Handbook of Experimental Psychology and Cognitive Neuroscience, Sensation, Perception, and Attention*, 4th ed. (John Wiley & Sons, 2018); Johan Wagemans, ed., *The Oxford Handbook of Perceptual Organization* (OUP Oxford, 2015); Mica Endsley et al., "Cognitive Engineering and Decision Making: An Overview and Future Course," *Journal of Cognitive Engineering and Decision Making* 1 (March 1, 2007): 1-21, https://doi.org/10.1177/155534340700100101.
77. David Gunning, "Explainable Artificial Intelligence (XAI)," DARPA, n.d., https://www.darpa.mil/program/explainable-artificial-intelligence.
78. Cliff Kuang, "Can A.I. Be Taught to Explain Itself?" *The New York Times,* November 21, 2017, sec. Magazine, https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html; Ariel Bleicher, "Demystifying the Black Box That Is AI," *Scientific American,* August 9, 2017, https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/; Paul Voosen, "How AI Detectives Are Cracking Open the Black Box of Deep Learning," Science | AAAS, July 5, 2017, https://www.sciencemag.org/news/2017/07/how-ai-detectives-are-cracking-open-black-box-deep-learning; Sara Castellanos and Steven Norton, "Inside Darpa's Push to Make Artificial Intelligence Explain Itself," WSJ (blog), August 10, 2017, https://blogs.wsj.com/cio/2017/08/10/inside-darpas-push-to-make-artificial-intelligence-explain-itself/; Will Knight, "The Dark Secret at the Heart of AI," *MIT Technology Review,* April 11, 2017, https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/.
79. Judea Pearl and Dana Mackenzie, *The Book of Why: The New Science of Cause and Effect* (Penguin UK, 2018).
80. MDDS Working Group, "Call for Absracts for Massive Digital Data Systems," November 3, 1993, https://groups.google.com/forum/#!topic/mail.cypherpunks/4CDiW59hS88; D. Parkins, "Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data," *The Economist* 413 (May 6, 2017), https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; Giovanni Navarria, Nick Couldry, and Rachell Li, "The Price of Connection: 'Surveillance Capitalism,'" The Conversation, September 23, 2016, http://theconversation.com/the-price-of-connection-surveillance-capitalism-64124; Bruce Schneier, "The Public/Private Surveillance Partnership," *Schneier on Security* (blog), August 5, 2013, https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html; Bruce Schneier, "Surveillance as a Business Model," *Schneier on Security* (blog), November 25, 2013, https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html; Jeff Nesbit, "Google's True Origin Partly Lies in CIA and NSA Research Grants for Mass Surveillance," *Quartz (*blog), December 8, 2017, https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/.
81. AT&T, "Transparency Report," accessed October 24, 2018, http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html; Google, "Transparency Report," Google, accessed October 25, 2018, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US; Verizon, "U.S. Report," Transparency Report, accessed October 24, 2018, https://www.verizon.com/about/portal/transparency-report/us-report/.
82. Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *The New York Times,* April 4, 2018, sec. Technology, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html; David Taylor, "Big Tech's Double Trouble: Political Heat from Trump and the Left May Signal Reckoning Ahead," *The Guardian,* September 2, 2018, sec. Technology, https://www.theguardian.com/technology/2018/sep/02/big-techs-double-trouble-bipartisan-criticism-may-signal-a-reckoning-ahead; Cate Cadell, "Facebook Plans Innovation Hub in China despite Tightening Censorship," *Reuters,* July 24, 2018, https://www.reuters.com/article/us-china-facebook-subsidiary/facebook-sets-up-subsidiary-in-china-filing-idUSKBN1KE1JF; Kate Conger, "Google Employees Resign In Protest Against Pentagon Contract," *Gizmodo* (blog), May 15, 2018, https://www.gizmodo.com.au/2018/05/google-employees-resign-in-protest-against-pentagon-contract/; John Naughton, "Wanted in the Digital Monopoly Age – Powers to Curb the Hold of Online Giants," *The Guardian,* September 16, 2018, sec. Opinion, https://www.theguardian.com/commentisfree/2018/sep/16/wanted-in-digital-monopoly-age-powers-to-curb-online-giants.
83. Robert McCreight, "Brain Brinksmanship: Devising Neuroweapons Looking at Battlespace, Doctrine, and Strategy," in *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns* (CRC Press, 2015), 118.
84. McCreight, "Brain Brinksmanship: Devising Neuroweapons Looking at Battlespace, Doctrine, and Strategy."

NOTES

85. Giordano, *Neurotechnology in National Security and Defense*; James J. Giordano and Bert Gordijn, *Scientific and Philosophical Perspectives in Neuroethics* (Cambridge University Press, 2010).
86. Zac Rogers, "The Geopolitics of Surveillance Capitalism," *Chesterfield Strategy* (blog), September 16, 2019, https://chesterfieldstrategy.com/2019/09/16/the-geopolitics-of-surveillance-capitalism/.
87. Martin Moore and Damian Tambini, *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press, 2018); Naughton, "Wanted in the Digital Monopoly Age – Powers to Curb the Hold of Online Giants."
88. Roger McNamee, "How to Fix Facebook—Before It Fixes Us," *Washington Monthly*, January 7, 2018, https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/; Nikhil Sonnad, "Everything Bad about Facebook Is Bad for the Same Reason," *Quartz* (blog), July 30, 2018, https://qz.com/1342757/everything-bad-about-facebook-is-bad-for-the-same-reason/.
89. Molly K. McKew, "Searching for a Stronghold in the Fight Against Disinformation," Centre for International Governance Innovation, June 4, 2018, https://www.cigionline.org/articles/searching-stronghold-fight-against-disinformation; Molly K. Mckew, "How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral," *POLITICO Magazine,* February 4, 2018, http://politi.co/2BSfTQ7; Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News* (HarperCollins, 2018).
90. Casey Newton, "Congress Just Showed Us What Comprehensive Regulation of Facebook Would Look Like," The Verge, July 31, 2018, https://www.theverge.com/2018/7/31/17632858/facebook-regulation-mark-warner-policy-paper-congress; Lina M. Khan, "Amazon's Antitrust Paradox," *The Yale Law Journal* 126, no. 3 (January 2017): 710-805; Taylor, "Big Tech's Double Trouble."
91. Adam Goldman, "Justice Dept. Accuses Russians of Interfering in Midterm Elections," *The New York Times*, October 20, 2018, sec. U.S., https://www.nytimes.com/2018/10/19/us/politics/russia-interference-midterm-elections.html.
92. Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *The New York Times*, September 20, 2018, https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.
93. Scott and Spaniel, *China's Espionage Dynasty.*
94. Ian Brown, "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust?" War on the Rocks, May 22, 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/; Neal A. Pollard, Adam Segal, and Matthew G. Devost, "Trust War: Dangerous Trends in Cyber Conflict," War on the Rocks, January 16, 2018, https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/; Rachel Botsman, *Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart* (Penguin UK, 2017).
95. Dmitri Trenin, "The Revival of the Russian Military: How Moscow Reloaded," F*oreign Affairs*, June 2016, https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/revival-russian-military; Mark Galeotti, "Heavy Metal Diplomacy: Russia's Political Use of Its Military in Europe since 2014" (European Council on Foriegn Relations, December 19, 2016), https://www.ecfr.eu/page/-/Heavy_Metal_Diplomacy_Final_2.pdf; Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016," 2016, http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf.
96. Nance, *The Plot to Destroy Democracy*; Scott and Spaniel, *China's Espionage Dynasty;* Robertson and Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies"; Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy."
97. Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton University Press, 2018).
98. Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times,* October 15, 2018, sec. Business Day, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.
99. Simina Mistreanu, "China Is Implementing a Massive Plan to Rank Its Citizens, and Many of Them Want In," *Foreign Policy*, April 3, 2018, https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.
100. Tiffany Li, "Opinion | China's Influence on Digital Privacy Could Be Global," *The Washington Post*, August 7, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/07/china-privacy/.
101. Paul and Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model."
102. Pomerantsev, *Nothing Is True and Everything Is Possible.*

NOTES

103. Jessica T. Mathews, "Power Shift," *Foreign Affairs*, February 1997, https://www.foreignaffairs.com/authors/jessica-t-mathews.
104. Steven Levy, *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age* (Penguin, 2001).
105. Terry Wagner, "Expertise and Disbelief: Post-1945 American Attitudes Toward the Authority of Knowledge" (LSU Doctoral Dissertation, 2015), http://digitalcommons.lsu.edu/cgi/viewcontent.cgi?article=2975&context=gradschool_dissertations; Jennifer Kavanagh and Michael D. Rich, "Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life" (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR2314.html?adbsc=social_TruthDecay_20180619_24130011&adbid=641487755088707174 4&adbpl=li&adbpr=165654; Jonathan D. Moreno, *The Body Politic: The Battle Over Science in America* (Bellevue Literary Press, 2011).
106. Nils Gilman, "The Twin Insurgency," T*he American Interest* (blog), June 15, 2014, https://www.the-american-interest.com/2014/06/15/the-twin-insurgency/.
107. P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell University Press, 2011); Lindsey Cameron and Vincent Chetail, *Privatizing War: Private Military and Security Companies Under Public International Law* (Cambridge University Press, 2013).
108. Benjamin J. Cohen, The Future of Money (Princeton University Press, 2004); Zac Rogers, "Blockchain and the State: Vehicle or Vice?" *Australian Quarterly*, March 2018.
109. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare.*
110. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
111. Katherine Mansted, "Activating People Power to Counter Foreign Interference and Coercion," Policy Options Paper (Canberra, ACT Australia: National Security College, ANU, December 2019), https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2019-12/pop_activating_people_power.pdf.
112. Khalilzad et al., *Strategic Appraisal: The Changing Role of Information in Warfare,* 36.
113. Clint Watts, "How About Some Unconventional Warfare? Thoughts On Countering ISIL," War on the Rocks, October 20, 2014, https://warontherocks.com/2014/10/how-about-some-unconventional-warfare-thoughts-on-countering-isil/; Clint Watts, "Advice for France in Its 'War on Terror,'" War on the Rocks, January 27, 2015, https://warontherocks.com/2015/01/advice-for-france-in-its-war-on-terror/; Clint Watts, "The Islamic State in Europe: Terrorists Without Borders, Counterterrorists With All Borders," War on the Rocks, March 29, 2016, https://warontherocks.com/2016/03/the-islamic-state-in-europe-terrorists-without-borders-counterterrorists-with-all-borders/.
114. Watts, *Messing with the Enemy.*
115. DARPA, "Social Media in Strategic Communication (SMISC)."
116. Waltzman, "A Center for Cognitive Security – Draft Proposal."
117. Waltzman.
118. See Reeder and Barnsby, "A Legal Framework Enhancing Cybersecurity through Public-Private Partnership," *The Cyber Defense Review*, Fall 2020, 31-45.
119. Emily Bienvenue and Zac Rogers, "Strategic Army: Developing Trust in the Shifting Strategic Landscape," *Joint Force Quarterly* 95 (November 2019): 4-14.
120. Zac Rogers, "158. In the Cognitive War – The Weapon Is You!" *Mad Scientist Laboratory* (blog), July 1, 2019, https://madsciblog.tradoc.army.mil/158-in-the-cognitive-war-the-weapon-is-you/.
121. Emily Bienvenue, Zac Rogers, and Sian Troath, "Trust as a Strategic Resource for the Defence of Australia," The Cove, October 29, 2018, https://www.cove.org.au/war-room/article-trust-as-a-strategic-resource-for-the-defence-of-australia/.
122. Josh Kerbel, "Coming to Terms with Anticipatory Intelligence," War on the Rocks, August 13, 2019, https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/.