Combined Information Overlay for Situational Awareness in the Digital-Anthropological Terrain

Reclaiming 'Information' for the Warfighter

Dr. Zac Rogers
Dr. Emily Bienvenue

INTRODUCTION

As noted in the 2019 *National Intelligence Strategy*,[1] technology-driven transformation across social, political, and economic domains continues at warp speed. Implications for militaries and their supporting Intelligence Community (IC) have expanded both in scope and complexity. Joint operational planning and evaluation occur in this disrupted and transitional environment, with very little predictable framework capable of guiding practitioners and strategists. This article addresses this discrepancy. The authors introduced and argued for creating a Strategic Engagement Specialist (SES) role in a JFQ article titled *Strategic Army* (October 2019), which concludes that strategic effect in the Information Environment (IE) cannot be achieved through discrete IOs, but rather, with holistic 'Strategic Engagement' that reinforces trust.[2] In that vein, here we introduce practical measures that should be incorporated into doctrine. The article addresses the following overarching questions: How can strategic intent more readily *translate* into a cross-enterprise approach to the IE and, how can that translation be made more discernible and actionable to enterprise-wide decision-makers? To this end, we describe the shortcomings of PMESII with IE shifts. Our proposed analytical framework and toolset augment existing approaches to situational awareness in the Digital Anthropological Terrain (DAT). We explain how scaffolding the operational framework with the Strategic Engagement approach, geared toward building human relationships, is the missing translation piece required to expedite successful IO integration within the Joint Military Appreciation Process (JMAP), and reflect on the implications for doctrine of adding the toolset and methodology we recommend.

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.

For the PMESII Problem

Operational and strategic planners are familiar with the political, military, economic, social, information, and infrastructure (PMESII) taxonomy. For four decades, analysis of PMESII taxonomies and their interplay have been the predominant analytical framework for the repeatable and timely assessment of the changing strategic landscape and operating environment. Indicative of the constant learning undertaken by the national security, intelligence, and defense (NSID) community during the Cold War, this framework seeks to capture the complexity of state behavior, treating states less like billiard balls and more like multi-faceted entities. It reflected the fact that the Cold War was a battle between whole societies for influence on and among the global order fought across multiple fronts. As Ducote notes in a 2010 School of Advanced Military Studies (SAMS) monograph, the basic PMESII schematic has been updated to PMESII-PT with the addition of "physical environment" and "time" and has been accompanied by an array of auxiliary and alternative frameworks favored by various branches of the NSID community.[3]

Traditionally, each category of analysis was treated as discrete, and each was assigned a branch of the NSID community responsible for that line of effort. A well-known wicked problem for organizations, this tended to obscure complex interactions across categories and almost blinded to emergent properties that arose from these interactions.[4] As Ducote explains, "Founders of PMESII sought knowledge to untangle the complicated aspects of a system. Then, they wanted to use their findings in the targeting process. However, they did not necessarily seek in-depth meaning and understanding about the complexity of a system."[5] As global complexity has markedly increased, particularly with the rise of digital technology and the hyper-connectivity it has enabled, the capacity for the NSID community to muddle through without suffering the serious risks of cognitive blind-spots is in question.[6] The strategic risk of

Dr. Emily Bienvenue, a Senior Analyst in Joint Operations and Analysis Division of the Defence Science and Technology Group where she provides support to strategic policy and operational planning, is also Adjunct and Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia.

making erroneous assumptions about the implications of complexity, and making hasty actions before fully understanding those implications is well documented.[7]

The growing awareness of adversarial Information Warfare (IW), and the flow of information through physical and human networks has provided a lens on this process. In practice, though, IW defaults to a means of achieving operational dominance in the physical battlespace through superior Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) with a precursor element of Psychological Operations (PsyOps). C4ISR technological dominance, especially in Cyber and Electronic Warfare (EW) operations, makes PsyOps, alongside the access and control over telecommunications infrastructure and media outlets for Information Operations (IOs), the standard means of producing informational effects under the catch-all of IW. Yet, as later explained, at the operational level these sporadic efforts fall short in the society-centric cognitive war.[8]

Society-centric, population-centric, and socio-cognitive political warfare, whether interruptions between outbreaks of kinetic Clausewitzian-organized violence or something more enduring, begins to overload the PMESII taxonomy and thus limits the practicality of defaulting to C4ISR dominance when it comes to IW. However enduring or episodic these shifts may be, a gap has opened up. (See Figure 1.)

Real-world examples of this gap are readily forthcoming. In the past 18 months, the NSID community, including Australia, was preoccupied with the contested balance of conventional military capabilities in the East Asian maritime periphery. Policy discussion and media commentary focused on expanding military and para-military maritime capabilities and island-building activities while academic research, and related issues were framed as a threat to conventional sea lane security.[9] Often characterized as “salami-slicing,” “little blue men"—the maritime equivalent of Russia's "little green men" in Crimea and Eastern Ukraine—inched their way forward in these waters, crisscrossed by strategically critical sea lanes, careful to avoid triggering the threshold of armed conflict. Maritime diplomacy was often pronounced as the solution to what was broadly understood as a geographically constrained traditional geopolitical struggle over a strategically important thoroughfare. This threat has also been analyzed within various IW contexts,[10] such as psychological, media, and legal, with the intent to sway public opinion and tip the scales in favor of adversarial narratives in various state-centric institutional forums.[11]

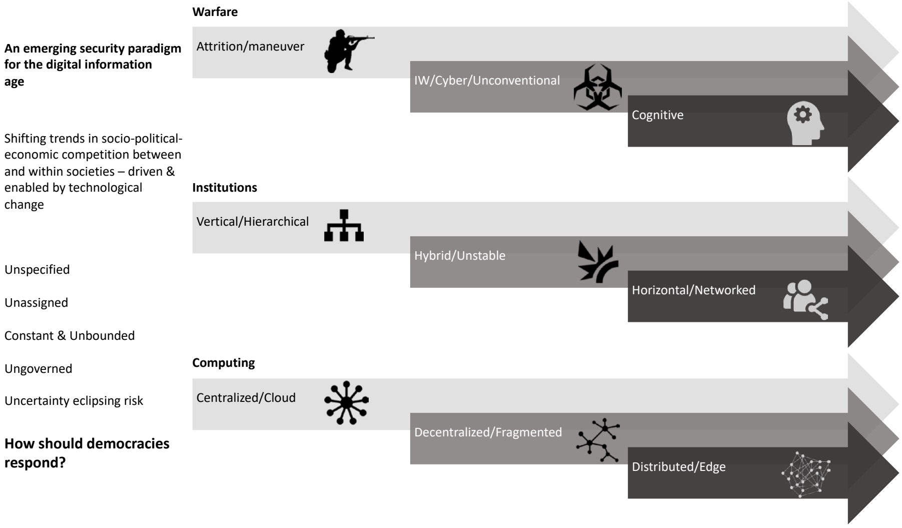

An emerging security paradigm for the digital information age
Shifting trends in socio-political-economic competition between and within societies – driven & enabled by technological change
Unspecified
Unassigned
Constant & Unbounded
Ungoverned
Uncertainty eclipsing risk
How should democracies respond?
Warfare
Attrition/maneuver
IW/Cyber/Unconventional
Cognitive
Institutions
Vertical/Hierarchical
Hybrid/Unstable
Horizontal/Networked
Computing
Centralized/Cloud
Decentralized/Fragmented
Distributed/Edge

Figure 1. Socio-Cognitive Security©

Retrospective analysis of the IE reveals a more fundamental change in the strategic landscape. At stake in the Indo-Pacific for Australia—beyond access to and control over this strategic maritime space—the socio-cognitive contest[12] playing out among regional populations. This contest is enabled by access to and control of a Digital Anthropological Terrain (DAT), which is now increasingly pivotal to peace and stability, or "the geopolitics of information" as one Australian analyst called it.[13] Similar dynamics characterize the Russian campaigns in Crimea, Eastern Ukraine, and across the Middle East.[14] Moreover, nation-states do not monopolize these trends. Various non-state actors are also exploiting the cognitive blind spots of Western NSID communities.[15] The offensive component of these society-centric cognitive warfare strategies is designed to undermine the social fabric of open societies, and thus the legitimacy of the rules-based governance of the commons –the foundation of US leadership and power since World War II.[16] It is also becoming clear that the defensive component is designed to sow enough confusion that it delays and disrupts a coherent, strategic response to this multi-faceted challenge. In practice, however, offensive and defensive components are unified via the fusion of effects facilitated by the participatory nature of digital space.[17]

The net effect benefits state and non-state actors who see fostering societal chaos as a feature, not a bug, of their strategic competition concept.[18]

As a recent study observed,[19] NSID communities seeking a battlefield knowledge edge find themselves embedded in a chaotic contest to unravel the *meaning* associated with that knowledge, and how it is formed and transmitted throughout society—something they are ill-equipped to do. Technology often fails to provide the answers that we seek.

Computers offer humans the promise of speed, efficiency, and precision in sorting and processing information, often at an unacknowledged cost. Providing these effects requires computers to *delete* information. Yet as humans have become socialized into new forms of human-computer interaction, we increasingly accept computational intervention as normal and warranted as it ascends the Cognitive Hierarchy.[20] Consistent with this cognitive schematic (See Figure 1.1.), we increasingly treat information as mere data, and knowledge as if were mere information. As each threshold dissolves, speed erodes the contextual boundaries between human understanding and statistical inference, leaving two residual consequences: creeping intellectual debt,[21] and paralyzing confusion.[22]

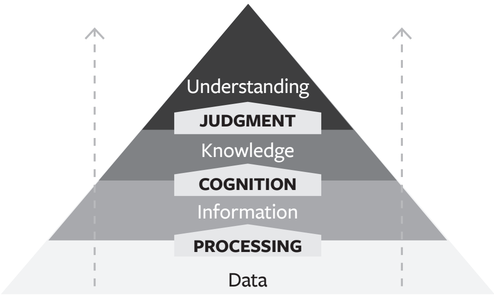


Figure 1.1. Cognitive Hierarchy

As the digital age has enveloped military affairs, and the deluge of data has driven the development of increasingly inscrutable sorting mechanisms known as deep-learning algorithms, humans are set to offload more and more of the cognitive process. Militaries labor under these conditions to pursue the conceptual development and practice of IO. In a 2002 SAMS monograph, Bryan Sparling highlighted a core question for the military in harnessing the digital information age: Are IO an *integration* strategy or are IO a *capability?*[23] The debate over this question remains unreconciled, with consequences that are accumulating. As Carl Builder noted in 1999, IO as an integration strategy implies a fundamental transformation of our military enterprise—new digital tools would not only alter military roles and missions; they would alter the primary purposeful activity of the modern military.[24]

IO as a capability implies an enterprise applying new tools to its existing roles and missions. As the answer to this question sorts out, militaries are hedging. In some cases, as Sean Lawson has observed, radical responses to the digital information age have been formulated and deployed on controversial intellectual foundations, with significant strategic consequences.[25]

Pre-empting this discrepancy in 2002, Sparling challenged the US DoD to "identify and articulate a relevant and theoretically sound definition of information before it can develop practical and effective doctrine for warfighting in the 21st century," asserting that IO must transcend the dichotomy of integration vs. capability.[26] Sparling's "Sentient Information Theory" urged DoD to interweave IO throughout the military enterprise and, crucially, to understand both the *internal* and *external* effects of this weaving.[27] In other words, as the military incorporates IO for effects in the world, IO will have effects on the military.

It is also safe to say the digital information age did not wait for such a definition to be socialized across the NSID. To date, while noted in the 2018 out-of-cycle *Joint Concept for Operating in the Information Environment* (JCOIE),[28] nothing like Sparling's recommendation has made its way into doctrine. Some analysts are alternatively recommending the concept of 'narrative warfare'.[29]

But is narrative warfare the appropriate paradigm? Ductote as a response to the PMESII problem urges "identity-based narration" in pursuit of holistic understanding of the OE. He too grapples with the fact that narrative warfare occurs across whole societies which are far more connected through horizontal networks, and thus, that all actions and activities taken by the NSID community and the military services are infused with a narrative whether intended or not. That is, the military may not be interested in narrative, but narrative is interested in the military.

These networks traverse an infrastructure that incorporates government organizations alongside commercial tech companies—media from the mobile device to the submarine cable. Dislocated from its traditional hierarchical position, the increasingly congested narrative warfare hosts fluid and deforming socio-political power structures in which the nation-state's traditional control power is scattered amidst competing mechanisms and processes causing constant perturbations.[30] For proponents of narrative warfare, the questions of narrative fratricide, blowback, and the unanticipated side effects of their interventions loom large. Should open democratic societies manipulate the manipulators? Game the gamers? And how would these measures impact the fabric of trust which is so vital to open society? As Kerbel puts it, this calls for states to engage in narrative warfare be an example of "activity masquerading as progress?"[31] And what other unintended consequences will come of such activity?

For NSID purposes, changes in the world require corresponding changes to the map and how it is produced and disseminated. The PMESII framework must be augmented to capture the disruptive social and political effects of rapid technological change to arm decision-makers with the timely, targeted information that reduces uncertainty. The digital age consists of an interactive medium that requires continuous up-to-date mapping and deconflicted operational planning that avoids informational fratricide[32] and otherwise achieves strategic alignment within defense organizations. As stated in *Military Strategy in the 21st Century:* "These interactions are not reducible to the physical confines of the land domain, which tend to focus on geography and terrain features. They represent a web of networks that define power and interests in a connected world. The state that best understands local contexts in all dimensions and builds a network around relationships harnessing local capacity is more likely to win the 21st-century struggle for the flanks."[33]

Practitioners agree. U.S. Army Cyber Brig. Gen. Richard Angle in July 2019 asserted the following:

> Army Cyber wants to enrich the concept of Multi-Domain Operations through the development of, or enhancing of, information warfare or maneuver in the Information Environment concept, and the further development, integration, and sync of information warfare capabilities across the full range of military operations in competition and conflict. (We are) expanding the concept of persistent engagement in cyberspace to persistent engagement in the Information Environment.[34]

Lt. Gen. Stephen Fogarty spoke of "a recognition that 1s and 0s moving in cyberspace are not necessarily turning things on or turning things off, but those 1s and 0s are moving information. And that information is changing behaviors and beliefs, and it more powerful than turning things on and turning things off."[35] If, after two decades of clarion calls, the NSID community is now resolved to embrace what many have framed as an imperative fraught with uncertainty, the NSID community must manage expectations of risk and opportunity and establish clear strategic goals in advance.

Situational Awareness in the Digital Anthropological Terrain (DAT)

Digital age situational awareness for planning, executing, and learning from military operations requires enhanced cartography. Systems and personnel at home or leaving domestic shores enter an environment comprised of the five familiar domains of land, sea, air, space, and cyberspace. Each of these domains has been carefully mapped using sophisticated ISR platforms, systems, and analysis designed to provide a dominating edge at the command level. Yet, as shown above, digital saturation and hyper-connectivity now link across these domains. This creates complex cross-domain interdependence and emergent properties and introduces non-linearity to the risk-uncertainty distinction thereby challenging prediction, preparedness, and resilience. Operational surprise can occur as a hostile narrative, easily prosecuted by fleeting, deniable, inexpensive, and increasingly automated tools.[36] Campaign failure can emerge from a growing range of sources, with the effect of reducing command and control to uncoordinated serial reactions to unexpected forces.

Incorporating the two "I's" of the PMESII taxonomy—infuses the other four domains, thereby improving situational awareness of the machinations of power and influence. Computer scientists, software engineers, network managers, and cybersecurity practitioners well understand the concept of digital stack. This concept has been further developed by theorists and analysts to better understand how technological, social, and political systems shift because of the digital information-networked age.[37] One chief architect of The Stack is Benjamin Bratton who captures this radically altered anthropological-technological global environment with a six-layered stack by describing it as a "semi-autonomous, accidental megastructure, governing but not governed, distorting and deforming contemporary political geographies."[38]

Many scholars before Bratton argued that digital technologies and human beings should be viewed as an enmeshed matrix of complex dependencies and relations instead of understood within the traditional instrumental human-technology schematic of "user" and "used."[39] Latour implored us to recognize the need to understand the human-technological domain broadly as an "anthropological matrix."[40] Science and technology historian George Dyson wrote of the emergence of "analogue computing," where digital computation merges with analogue human behaviors in unpredictable and radical ways.[41] This discourse, with specific reference to the digital age and operational military affairs, leads us to assign a Digital Anthropological Terrain (DAT).

We seek to re-establish a foothold for operators plagued by uncertainty and to connect operations to strategy. Our response falls somewhere between recommendations by Sparling and Ducote in their 2002 and 2010 SAMS monographs. We aim to respond conservatively, judiciously, and defensively to the foregoing developments without advocating for the implementation of measures that increase the risks of narrative fratricide, blowback, and lost trust. We utilize the digital stack theme to develop an operationally-focused Combined Information Overlay (CIO) to augment the strategic multi-layered analysis of the Digital Anthropological Terrain (See Figure 1.2.). As a framework to map distorted and deformed flows of information and power in any digitally saturated environment, it can aid in augmenting PMESII. The digital stack layers are sites of major consequence—pivotal gateways accommodate influential gatekeepers that control information flow across the digital stack. As a stepping-stone, these sites of cyber-enabled influence are analogous to air-sea-land bubbles—A2/AD pockets whereby a superior conventional joint military force or coalition of forces could seek to exert temporal and spatial denial or control of traffic transiting the relevant zone.[42]

The historical analogy with familiar air-sea-land domains and the will and capacity of states to deny and control these commons only extends so far into cyberspace.[43] *States* face not only a greater diversity of agents both resolved and capable of challenging denial and control of the DAT and the structure of the digital commons, which lends itself to vastly greater exploitation. Loudoun County,[44] Virginia which, according to its economic-development board, still routes 70-80 percent of global internet traffic,[45] acts as a digital age Strait of Hormuz in terms of control of the commons, but this analogy is superficial. Translating control into strategic gain is more complex and protean when it comes to information. When crude oil hits the marketplace, the forces of supply and demand assume control—US and allied national security apparatus perform their primary strategic job once extraction, processing, and transit are secured.

In contrast, when digital information hits the marketplace, a wide and ever-shifting range of agents and structures take over. Contrary to many popular accounts, data is not the new oil.[46]

The supply chains associated with the hardware and software that constitute the digital medium are global, complex, unprotected, and vulnerable. Digital infrastructure from submarine cable landing points to regional telecommunications hubs and local cellular networks is diverse and exploitable. The last 12 inches of the DAT—the human-computer interface—is a congested zone of manipulation employing insights from the cognitive and behavioral sciences for a range of commercial and political ends, both legitimate and nefarious.[47] The implications of this caldron are only beginning to be understood in terms of impact on socio-political stability,[48] human well-being,[49] and the democratic fabric.[50] Military effectiveness—which ultimately draws all of its resources from society[51] and is continuously impacted by all societal changes—is deeply implicated.[52] This means serious augmentation of PMESII for the digital age is critical.

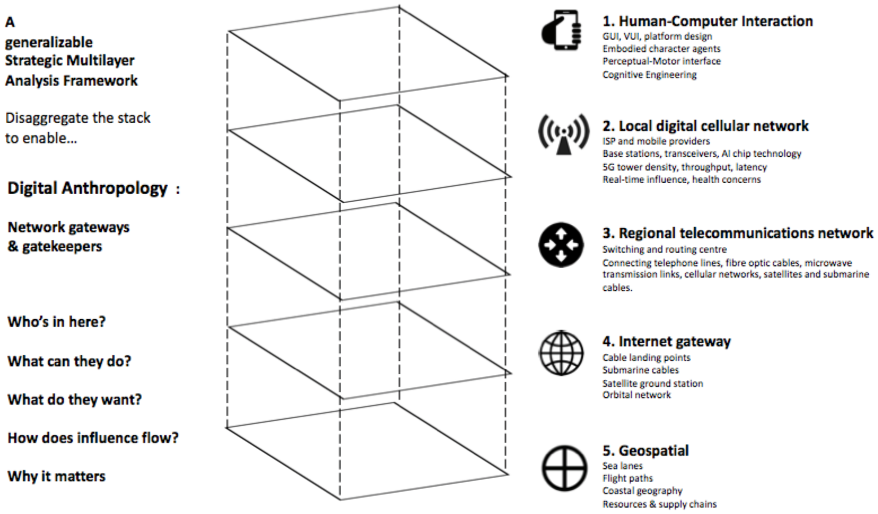

A
generalizable
Strategic Multilayer
Analysis Framework
Disaggregate the stack
to enable...
Digital Anthropology :
Network gateways
& gatekeepers
Who's in here?
What can they do?
What do they want?
How does influence flow?
Why it matters
1. Human-Computer Interaction
GUI, VUI, platform design
Embodied character agents
Perceptual-Motor interface
Cognitive Engineering
2. Local digital cellular network
ISP and mobile providers
Base stations, transceivers, AI chip technology
5G tower density, throughput, latency
Real-time influence, health concerns
3. Regional telecommunications network
Switching and routing centre
Connecting telephone lines, fibre optic cables, microwave transmission links, cellular networks, satellites and submarine cables.
4. Internet gateway
Cable landing points
Submarine cables
Satellite ground station
Orbital network
5. Geospatial
Sea lanes
Flight paths
Coastal geography
Resources & supply chains

Figure 1.2. Digital Trust©

Disaggregating the DAT

The operation of five digital stack surfaces are both individually consequential, and are also a component of the whole, making the analyst's role pivotal. Adding the digital stack to PMESII brings operational analysis and planning up to speed with the existing operationally important (but still under-appreciated) phenomena; it also will enable foresight in the radically shifting landscape of power and influence the NSID community needs to operate within. The first step in producing a Combined Information Overlay needed for analysis in operational planning and evaluation happens by populating the surfaces described below with information. Open-source information relevant to these surfaces is abundant and should not be overlooked. Once populated, and depending on the nature of the corpus developed, various data tools can help identify sites of unexpected and highly useful information not captured by the PMESII approach. These tools range from a simple web crawler to patterns of connection identified in digital trace data[53]—URLs, social media posts, and threads—to more sophisticated digital forensic tools that work with unstructured data to produce statistical inference. The resulting CIO will augment PMESII and assist the strategic analyst who ideally would be proximal across the decision-making structure. As explained below, the analyst populating the stack with information must be mindful of the terrain.

Surface 1. Human-Computer Interface (HCI)

The last 12 inches is the most tactically pivotal and fast-moving surface of the DAT. Humans interact with computers in many ways; the design interface between humans and computers is crucial to facilitating this interaction and has been a growing industry since the mid-1990s.[54] Desktop applications, internet browsers, every conceivable platform and application on now-ubiquitous handheld mobile devices make use of the graphical user interfaces (GUI) of today. Voice user interfaces (VUI) are used for speech recognition and synthesizing systems, and the emerging multi-modal interfaces allow humans to engage with embodied character agents and virtual assistants in ways not possible with other interface paradigms. HCI has grown insofar as quality of interaction, and in different branching of the purposes of interactions. Instead of designing regular interfaces, the different research branches have focused on different aspects of concepts of multimodality, intelligent adaptive interfaces, and, active interfaces. Each branch is fed continuously with insights and developments emerging from the cognitive sciences over more than three decades.[55] Innovation is supercharged by dual-use commercial incentives, which keeps political warfare practitioners far ahead of the government's regulatory and legislative oversight. Command and control must be aware and prepared for adversaries to manipulate, cognitively affecting personnel serving during operations and also on the home front. Measures to protect information assurance between command and personnel—such as repudiable digital record of authenticity using technologies such as blockchain—are readily available.

Surface 2. Local Digital Cellular Network

This surface represents the highly critical last few hundred feet in adversary IO targeting populations. Digital cellular networks are divided into a mosaic of small geographical areas, or cells. Sound and image analog signals are digitized in the mobile device, converted by an analogue-to-digital converter, and transmitted as a stream of bits. All wireless devices in a cell communicate by radio waves with a local antenna array and low-power automated transceiver (transmitter and receiver), over frequency channels assigned by the transceiver from a common pool of frequencies, which are reused in geographically separated cells. Local antennas relate to the telephone network and the Internet by a high-bandwidth optical fiber or a wireless backhaul. Like existing cellphones, when a user crosses from one cell to another, their mobile device is automatically handed off to the antenna in the new cell. The corporate gatekeepers of technology ownership and administration in these networks are critical, and the supply chain of technological components that make the network function are critical to both offensive and defensive influence. Sound data analysis of API nodes at this surface improves the situational awareness of attempts to manipulate or distort the IE.

Surface 3. Regional Telecommunications Network Backbone

This critical operational surface in terms of routing and switching is the backbone of the regional telecommunications network. It includes telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers facilitating communication among most devices. Originally a network of fixed-line analogue telephone systems, in many countries the backbone is now almost entirely digital at its core and includes mobile and other networks, as well as fixed telephones. Again, ownership and administration of this surface is a critical gateway for routing information to sections of the population targeted for influence. Developing nation-states seeking to enter the digital age are particularly vulnerable to undetected hostile influence that invades the DAT. Commands here can incorporate knowledge of hardware ownership and administration to enhance operational risk awareness and gauge the extent to which regional IT infrastructure is trustworthy.

Surface 4. Internet Gateway

This slower moving, foundational surface is a network of private, public, academic, business, and government networks of local or global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web, electronic mail, telephony, and file sharing. Where the nation-state connects to the global Internet via a cable landing station and the cable itself, and in under-developed and sparsely populated archipelagic regions in particular, local satellite infrastructure is obviously a critical gateway with huge operational implications for those who own and administer these technologies.

Surface 5. Geospatial

Geospatial is the strategic surface with the greatest inertia. The increasing ability to capture geographic data is creating an increasingly data-rich environment, including remotely sensed imagery, environmental monitoring systems such as intelligent transportation systems, and location-aware technologies such as mobile devices that report location in near real-time. A geographic information system (GIS) provides platforms for managing these data, computing spatial relationships such as distance, connectivity, and directional relationships between spatial units, and visualizing both the raw data and spatial analytic results within a cartographic context. Also, basic DAT components are dispersed geospatially. The extraction, processing, and transporting of rare earth minerals, and the manufacturing processes to which these minerals are critical inputs, such as the semi-conductor industries which dot the East Asian maritime periphery, represent the geospatially dispersed DAT. Security and control at this surface are strategic imperatives for the relevant operational command.

DAT Denial vs. DAT Control?

While the DAT cannot be wholly controlled by command, freedom of maneuver can be denied to hostile narratives. Great improvement can be achieved here by the military. By way of analogy, sea denial and sea control are long- and well-understood naval concepts.[56] For navies, sea denial is the denial of a certain maritime domain to an adversary, with or without access and transit of such area for oneself, whereas sea control denotes the achievement of both. Generally, sea denial is much more readily achievable than sea control, particularly in the era of precision-strike parity.[57] Sea control may be grasped temporarily during major combat operations but usually cedes to sea denial as forces demobilize and seafarers fall back on a constabulary presence.

The denial versus control contrast deepens in cyberspace to the point of redundancy. DAT control—the capacity to deny digital-anthropological medium usage while freely using the terrain unharried—is nearly impossible, even during major cyber operations. Advocates of engagement in narrative warfare must be able to account for indiscrete boundaries of their interventions, and the consequences of their interventions are multi-directional. Side effects and accidents are unavoidable when intervening in complex anthropological systems—the sciences offer nothing to eliminate this reality. This constraint, and an open society's heavy reliance on trust as a foundational societal imperative, means that narrative warfare that seeks to manipulate a given section of the population requires a rigorous cost-benefit analysis of long-term strategic effects and a serious dose of prudence and realism.

DAT denial—the capacity to deny free use of the medium to an adversary while not being free to use it unharried—is a much more plausible goal. DAT denial holistically is the force's foundation of operational cognitive security. Understanding how influence operates through the DAT helps to identify opportunities to deny access to adversaries and gain a small window of advantage. It does not mean offensive cognitive operations always succeed. Information fratricide, the well-established failure rate of covert interventions,[58] and the emerging ethical constraints on increasingly transparent warfare[59] present high barriers to ambitions of DAT control. A better approach is to use DAT denial to pursue resilient human relationships by cultivating and reinforcing trust. The authors echo Sparling in advocating for leveraging trust as a heuristic for Strategic Engagement allows information to be wielded not as a narrative weapon but rather to cultivate our preferred environmental condition. Yet the bluntest and generally counterproductive example of DAT denial is an Internet blackout—and states often have opted for this lose-lose option.[60] It serves, however, as a glimpse of near-future conflict. Augmenting operational security with analogue civil-military human relationships long-term is a win-win. When the lights go out, what else does the enterprise fall back on?

Integrating the DAT into JMAP for Strategic Engagement

JMAP acknowledges Phase Zero scoping and shaping must intersect the phases. The need for persistent engagement under the Accelerated Warfare concept is the most explicit official acknowledgment of this.[61] By augmenting PMESII with CIO for situational awareness in the DAT, we provide a structured way to address complexity in the form of recurring updatable analysis with immediate relevance to the decision-maker. As for the JMAP (See Figure 1.3), an in-practice disconnect remains in the ways the arrows connecting Joint Intelligence Preparation for the OE impact on decision-making across the phases, how those decisions connect and align with strategic intent, and how the feedback loops across the phases arm the decision-maker with meaningful information about the operation. Lots of information gets exchanged, but the decision-maker is often left asking "so what?" What is the plot binding each decision, what is the narrative signature that each decision creates?

Strategic Engagement Specialist
(SES)
role

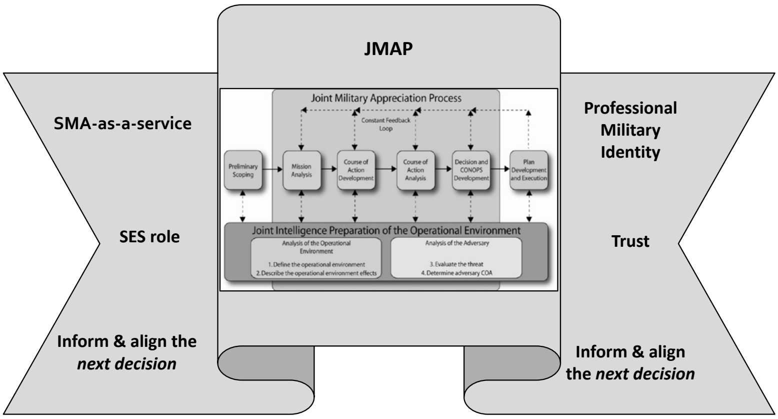
Use **DAT-denial** to mitigate adversarial narratives

Use **Combined Information Overlay** for **SMA** to equip decision-makers for Strategic Engagement

Augment **Strategic Engagement** with face-to-face trust building and sustainment

Align strategic & operational objectives at each decision point across the enterprize by…

Prioritizing **professional military identity** to connect strategic intent with **information as an environmental condition**


JMAP
SMA-as-a-service
SES role
Inform & align the *next decision*
Professional Military Identity
Trust
Inform & align the *next decision*
Joint Military Appreciation Process
Constant Feedback Loop
Preliminary Scoping
Mission Analysis
Course of Action Development
Course of Action Analysis
Decision and CONOPS Development
Plan Development and Execution
Joint Intelligence Preparation of the Operational Environment
Analysis of the Operational Environment
1. Define the operational environment
2. Describe the operational environment effects
Analysis of the Adversary
3. Evaluate the threat
4. Determine adversary COA

"information as an environmental condition"

Figure 1.3. SMA-as-a-service©

Strategic Engagement is not realized until these arrows inform the decision-maker of key and digestible information. This can be produced in the form of CIO for situational awareness in the DAT, but the question "So what?" remains. This question is answered by referring to DAT denial as the *persistent operational objective* and trust-building as the *environmental condition*[62] in which strategic intent is pursued. DAT denial and trust connect operational and strategic levels, with the aim of elucidating and facilitating an all-enterprise understanding, as urged by Sparling.

Analysts who exchange OE intelligence with practitioners, and practitioners who cross-reference operational status can access a common understanding of the desired environmental condition of information without requiring an identical flow of intelligence and without receiving identical orders simultaneously from command. Trust as a strategic resource underpins the preferred environmental condition and DAT denial as the preferred operational state. These are the connective tissues that need strengthening in the existing JMAP as it is currently practiced.

Bolstering Professional Military Identity as a Strategic Resource

The role trust plays in today's strategic landscape speaks to the importance of honor and integrity in professional military identity and how the integrity of our service professionals serves as a key ingredient in the fight to protect our democratic societies. Traditionally, our military has been one of our most trusted institutions. in Western democratic societies, and this remains true today. A 2018 Gallup study showed 74 percent of Americans polled trusted the military "a great deal or quite a lot"– the highest of all institutions.[63] Military professionals are at the coalface of international diplomacy in an era of radical transparency and contested narrative, and so is the foundational backstop of strategic trust. Acknowledgment of such is needed to precipitate greater investment in professional military education to capitalize on values of honor and integrity—a natural strength of the military enterprise—as our best defense against the malign information campaigns of our adversaries.

Professional military identity, a strategic resource, can also help bridge the gap between the strategic integration of IO across the military enterprise and operational decision-making, planning, and evaluation. Tactical technological advances and innovative organizational reform can only get the enterprise so far. The last six inches—the "so what" question confronting the operator amidst a deluge of information, knowledge, and narrative—remains vulnerable to the stifling and paralyzing effects of uncertainty in the cognitive battlespace. Technological and organizational mitigations are necessary but insufficient in the cognitive war. Cognitive security is a construction of the originator—a narrative pushed forward as much as one deduced from the IE. Noting that technological and organizational fixes will never be sufficient even with improvement over time, the key to finding a foothold in the digital age and reclaiming information for the warfighter are the values and identity of the originator with no other choice except to operate in a protean and fluid IE. As noted above and argued for in *Strategic Army*, the military's status, particularly the Army as the societal trusted institution *sine qua non*, is the heuristic around which IO integration at both the strategic and operational levels should be pursued.

CONCLUSION

This article addresses the following questions: How can strategic intent more readily *translate* into a cross-enterprise approach to the IE, and how can that translation be made more discernible and actionable, enterprise-wide, to decision-makers? These are not simple tasks. For more than two decades, scholars and practitioners have underscored the imperative for the military enterprise to adapt to the digital age. The armed forces and their supporting NSID communities have yet to reach the optimum stage where, as Sparling urges, terms and concepts such as IO, IW, and IE are made redundant because the entire military enterprise understands "information" as an *environmental condition*, in the way a seafarer understands seawater or an infantryman the landscape's topography. The CIO introduced here for situational awareness in the DAT represents an overdue retracing of steps for the military with emphasis on operational security in cognitive war. It should by now be uncontroversial to recognize that the primary contest in cognitive war, as members of the NSID community, is with ourselves.[64]

But the perennial strategic question is clear: What *conditions* should we be seeking to establish? And, operationally, how should those conditions lead towards the next decision? The fusing of approaches to information in operations and strategy in the digital age cannot succeed without incorporating the way that the originators' operations and strategy create a narrative signature, and how audiences read and receive that signature. The hyper-connected digital age means the audience is global, the signature is mutable and travels at light speed, and control power in the DAT is an increasingly dangerous and self-defeating fantasy. Operators need a foothold for operational security grounded in cognitive security throughout meaningful activities. This means persistence and conservative expectations about how the DAT can be managed.

Digital age realities mean the construction and maintenance of analogue human relationships, in which trust is established as a strategic resource rather than an auxiliary luxury, will remain critical to operational success in the digital age. DAT denial that accompanies human relationships is a capability—its significance to the strategic integration of information across the enterprise is in its proximity to trust as the critical missing translation piece.

Trust in this context is akin to an environmental condition the originator seeks to attain and sustain, not a signature it seeks to exploit. Trust is defendable precisely because it weaves in and out of the human-machine terrain in indiscrete, culturally specific ways. Those seeking to abuse trust and employ it offensively in cyberspace will encounter this constraint. We achieve operational security in the cognitive domain by pushing trust forward not by retreating from it in a race to the bottom with an adversary for whom trust is a non-starter. To this end, we view DAT denial via constantly updated and disseminated CIO; using the framework outlined here should be part of the enterprise-wide doctrine. The JMAP needs an overhaul, not mere augmentation, aligning operations and strategy with an information-relevant environment, thereby reclaiming information for the warfighter. Cultivating and sustaining trust in human relationships strategically aligns the enterprise, and renders it accessible and understandable for decisionmakers at every level. Trust is the core "plot" binding every narrative signature. IO without trust will continue to oscillate between self-defeating and costly at the operational level and will be dangerously corrosive at the strategic level.

DISCLAIMER

The views expressed below are the authors', and do not represent the official view of the Australian Defense Department.

NOTES

1. Office of the Director of National Intelligence, "National Intelligence Strategy of the United States of America" (United States Intelligence Community, 2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.
2. Emily Bienvenue and Zac Rogers, "Strategic Army: Developing Trust within the Cognitive Battlespace," DST Group Discussion Paper (Edinburgh, South Australia: Joint Operations and Analysis Division, DST Group, 2018).
3. Brian M. Ducote, "Challenging the Application of PMESII-PT in a Complex Environment" (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2010), 2-5, https://apps.dtic.mil/dtic/tr/fulltext/u2/a523040.pdf.
4. The literature on 'emergence' in complex systems is enormous for a good introduction see Harold J. Morowitz, *The Emergence of Everything: How the World Became Complex* (Oxford University Press, USA, 2002); John H. Holland, *Emergence: From Chaos to Order* (Oxford University Press, 2000); Lars-Erik Cederman, *Emergent Actors in World Politics: How States and Nations Develop and Dissolve* (Princeton University Press, 1997); Ducote's primary influence is Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity : A Platform for Designing Business Architecture* (Butterworth-Heinemann, 2006).
5. Ducote, "Challenging the Application of PMESII-PT in a Complex Environment," 6.
6. Zachery Brown, "Librarians of Babel: Intelligence's Three Big Problems in the Information Age," Real Clear Defense, December 5, 2018, https://www.realcleardefense.com/articles/2018/12/05/librarians_of_babel_intelligences_three_big_problems_in_the_information_age_114003.html; Zachery Brown, "What Would You Say You Do Here? Redefining the Role of Intelligence in the Information Age," War on the Rocks, December 5, 2018, https://warontherocks.com/2018/12/what-would-you-say-you-do-here-redefining-the-role-of-intelligence-in-the-information-age/.
7. Sean T. Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Routledge, 2013).
8. US Army, FM 3-13 (FM 100-6), *Information Operations: Doctrine, Tactics, Techniques, and Procedures, November 2003* (CreateSpace Independent Publishing Platform, 2012).
9. ANDREW S. ERICKSON, "America's Security Role in the South China Sea," *Naval War College Review* 69, no. 1 (2016): 7-21; Peter Dutton, Andrew S. Erickson, and Ryan Martinson, "China's Near Seas Combat Capabilities" (China Maritime Study, Number 11) (DTIC Document, 2014), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA612569.
10. Nathan Freier et al., "Outplayed: Regaining Strategic Initiative in the Gray Zone" (Carlisle, PA: Army War College, 2016), http://www.dtic.mil/docs/citations/AD1013807; Douglas Lovelace, Hybrid Warfare and the Gray Zone Threat (Oxford: Oxford University Press, 2016).
11. Liang Qiao and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America* (NewsMax Media, Inc., 2002); M. Taylor Fravel, "China's Strategy in the South China Sea," *Contemporary Southeast Asia* 33, no. 3 (December 2011): 292-319; M. Taylor Fravel, "Power Shifts and Escalation: Explaining China's Use of Force in Territorial Disputes," *International Security* 32, no. 3 (January 1, 2008): 44-83, https://doi.org/10.1162/isec.2008.32.3.44; M. Taylor Fravel, "Regime Insecurity and International Cooperation: Explaining China's Compromises in Territorial Disputes," *International Security* 30, no. 2 (2005): 46-83.
12. 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; 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/.
13. Katherine Manstead and Eric Rosenbach, "The Geopolitics of Information," Belfer Center for Science and International Affairs, May 28, 2019, https://www.belfercenter.org/publication/geopolitics-information; Katherine Manstead, "The Revenge of Geography in Cyberspace," The Strategy Bridge, June 4, 2019, https://thestrategybridge.org/the-bridge/2019/6/4/the-revenge-of-geography-in-cyberspace.

14 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/.

15. Shima D. Keene, "Silent Partners: Organized Crime, Irregular Groups, and Nation-States" (Strategic Studies Institute, US Army War College, October 23, 2018), https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1392.

NOTES

16. Barry R. Posen, "Command of the Commons: The Military Foundation of US Hegemony," *International Security* 28, no. 1 (2003): 5-46.
17. Alicia Wanless and Michael Berk, "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications," ResearchGate, accessed February 6, 2019, https://www.researchgate.net/publication/329281610_Participatory_Propaganda_The_Engagement_of_Audiences_in_the_Spread_of_Persuasive_Communications; Zac Rogers, Emily Bienvenue, and Maryanne Kelton, "The New Age of Propaganda: Understanding Influence Operations in the Digital Age," *War on the Rocks*, May 1, 2019, https://warontherocks.com/2019/05/the-new-age-of-propaganda-understanding-influence-operations-in-the-digital-age/.
18. Timothy Thomas, "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations," *Defence Strategic Communications* 1, no. 1 (2015): 11-24; Timothy L. Thomas, *Decoding The Virtual Dragon Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy The Art Of War And IW* (Foreign Military Studies Office, 2007).
19. "SMA White Paper: What Do Others Think and How Do We Know What They Are Thinking?" A Strategic Multilayer Assessment Periodic Publication (DoD, Joint Chiefs of Staff, March 2018), http://nsiteam.com/social/wp-content/uploads/2018/03/White-Paper_What-Do-Others-Think_March2018_FINAL.pdf.
20. Department of the Army, "FM 100-6 Information Operations" (Washington D.C., Office of the Chief of Staff of the Army, 1996), 100.
21. Jonathan Zittrain, "The Hidden Costs of Automated Thinking," *The New Yorker*, July 23, 2019, https://www.newyorker.com/tech/annals-of-technology/the-hidden-costs-of-automated-thinking; D. Sculley et al., "Machine Learning: The High Interest Credit Card of Technical Debt," in *SE4ML: Software Engineering for Machine Learning* (NIPS 2014 Workshop), 2014, https://ai.google/research/pubs/pub43146.
22. Charles Kriel, "Fake News, Fake Wars, Fake Worlds," *Defence Strategic Communications* 3 (2017): 171-190.
23. Bryan Sparling, "Information Theory as a Foundation for Military Operations in the 21st Century" (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2002), https://apps.dtic.mil/dtic/tr/fulltext/u2/a403845.pdf.
24. Carl H. Builder, "The American Military Enterprise in the Information Age," in *Strategic Appraisal: The Changing Role of Information in Warfare* (RAND Corporation, 1999), https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap2.pdf.
25. Lawson, *Nonlinear Science and Warfare.*
26. Sparling, "Information Theory as a Foundation for Military Operations in the 21st Century," 2002, iii.
27. Sparling, 45.
28. Joint Chiefs of Staff, "Joint Concept for Operating in the Information Environment (JCOIE)" (Department of Defense, July 25, 2018), 12-13, https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.
29. 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/.
30. Peter J. Katzenstein and Lucia A. Seybert, "Protean Power and Uncertainty: Exploring the Unexpected in World Politics," *International Studies Quarterly* 62, no. 1 (March 1, 2018): 80-93, https://doi.org/10.1093/isq/sqx092.
31. 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/.
32. Information fratricide is defined as "the result of employing information operations elements in a way that causes effects in the information environment that impede the conduct of friendly operations or adversely affect friendly forces, U.S. Army, *FM 3-13 (FM 100-6) Information Operation*s.
33. Charles Cleveland, Benjamin M. Jensen, and Susan Bryant, *Military Strategy for the 21st Century: People, Connectivity, and Influence* (Cambria Press, 2018).
34. Bill Roche, "Summit Helps Chart Way Ahead for Maneuver in Information Environment," www.army.mil, August 7, 2019, https://www.army.mil/article/225430/summit_helps_chart_way_ahead_for_maneuver_in_information_environment.
35. Roche.

NOTES

36. Glenn Greenwald, “How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations,” *The Intercept* (blog), February 24, 2014, https://theintercept.com/2014/02/24/jtrig-manipulation/; Fred Adkins and Shawn Hibbard, “The Coming Automation of Propaganda,” *War on the Rock*s, August 6, 2019, https://warontherocks.com/2019/08/the-coming-automation-of-propaganda/.
37. Luciano Floridi, T*he Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford University Press, 2014); Seb Franklin, *Control: Digitality as Cultural Logic* (MIT Press, 2015); David Golumbia, *The Cultural Logic of Computation* (Harvard University Press, 2009); D. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (Springer, 2015); Duncan J. Watts, Six Degrees: The Science of a Connected Age (Random House, 2004).
38. Benjamin H. Bratton, *The Stack: On Software and Sovereignty* (MIT Press, 2016).
39. Ian Hodder, *Entangled: An Archaeology of the Relationships Between Humans and Things* (John Wiley & Sons, 2012); Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (University of Chicago Press, 2010); David Livingstone, *Transhumanism: The History of a Dangerous Idea* (David Livingstone, 2015).
40. Bruno Latour, “Technology Is Society Made Durable,” *The Sociological Review* 38, no. 1,suppl (May 1, 1990): 103-31, https://doi.org/10.1111/j.1467-954X.1990.tb03350.x; Bruno Latour, “How to Write the Prince for Machines as Well as for Machinations,” in Technology and Social Process (Edinburgh University Press, 1988).
41. George Dyson, *Turing’s Cathedral: The Origins of the Digital Universe* (Penguin UK, 2012); George Dyson, “Childhood’s End,” Edge (blog), January 1, 2019, https://www.edge.org/conversation/george_dyson-childhoods-end.
42. Popularized from 2010 onwards in the discourse on Air Sea Battle; see Jan Van Tol et al., “AirSea Battle: A Point-of-Departure Operational Concept” (Washington, D.C.: Center for Strategic and Budgetary Assessments, May 2010), http://www.csbaonline.org/publications/2010/05/airsea-battle-concept/; Andrew F. Krepinevich, “Why AirSea Battle?” (Washington: Center for Strategic and Budgetary Assessments, February 2010), http://www.csbaonline.org/publications/2010/02/why-airsea-battle/; Andrew F. Krepinevich, “The Future of U.S. Defense Strategy and the Japan-U.S. Alliance” (June 23, 2015), http://csbaonline.org/2015/06/23/the-future-of-u-s-defense-strategy-and-the-japan-u-s-alliance/.
43. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar What Everyone Needs to Know (*New York: Oxford University Press, 2014).
44. Paul E. Ceruzzi, *Internet Alley: High Technology in Tysons Corner*, 1945-2005 (MIT Press, 2008).
45. Sarah Price, “Loudoun, Virginia’s Data Center Alley: Computing Power of 10 Million Servers at Plug-and-Play Price,” *Loudoun County Economic Development, VA* (blog), January 4, 2019, https://biz.loudoun.gov/2019/01/04/loudoun-virginias-data-center-alley-computing-power-of-10-million-servers-at-plug-and-play-price/.
46. “The World’s Most Valuable Resource Is No Longer Oil, but Data,” *The Economist,* May 6, 2017, https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource; Ioanna D. Constantiou and Jannis Kallinikos, “New Games, New Rules: Big Data and the Changing Context of Strategy,” *Journal of Information Technology* 30, no. 1 (March 1, 2015): 44-57, https://doi.org/10.1057/jit.2014.17; Zac Rogers, “Data Is Not the New Oil; Data Is the New Sea,” *The Fox and the Grapes* (blog), May 17, 2017, https://thefoxandthegrapesblog.wordpress.com/2017/05/17/data-is-not-the-new-oil-data-is-the-new-sea/.
47. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).
48. Andrew Keen, *Digital Vertigo: How Today’s Online Social Revolution Is Dividing, Diminishing, and Disorienting Us* (St. Martin’s Press, 2012).
49. Douglas Rushkoff, *Team Human* (New York: W.W. Norton & Company, 2019).
50. Martin Moore, *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age* (Oneworld Publications, 2019).
51. Peter Layton, “Social Mobilisation in a Contested Environment,” The Strategist, August 5, 2019, https://www.aspistrategist.org.au/social-mobilisation-in-a-contested-environment/.

NOTES

52. Christopher Sims, "The Military and the Internet: Will War as We Know It Become Outmoded?" *Modern War Institute* (blog), July 18, 2019, https://mwi.usma.edu/military-internet-will-war-know-become-outmoded/; Sebastien Bay and Nora Biteniece, "The Current Digital Arena and Its Risks to Serving Military Personnel," Responding to Cognitive Security Challenges (Latvia: NATO STRATCOM COE, January 2019), https://stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel.
53. Rob Ackland and Zac Rogers, "Mapping Australia's Blockchain Ecosystem: Insights from Digital Trace Data" (April 18, 2019).
54. Julie A. Jacko, *Human Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications,* Third Edition (CRC Press, 2012); B.J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (Morgan Kaufmann, 2003); Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge: Harvard University Press, 2018).
55. National Research Council et al., *Emerging Cognitive Neuroscience and Related Technologies* (National Academies Press, 2008); 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).
56. Robert Rubel, "Talking about Sea Control," *Naval War College Review* 63, no. 4 (2010), https://digital-commons.usnwc.edu/nwc-review/vol63/iss4/6.
57. Randy Huiss, "Proliferation of Precision Strike: Issues for Congress" (Congressional Research Service, May 14, 2012), http://fas.org/sgp/crs/nuke/R42539.pdf.
58. Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2018); Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ : Princeton University Press, 2018).
59. George R. Lucas, Jr., *Ethics and Military Strategy in the 21st Century: Moving Beyond Clausewitz* (Routledge, 2019).
60. Katie Collins, "Ukraine Blackout Is a Cyberattack Milestone," CNET, January 5, 2016, https://www.cnet.com/news/cyberattack-causes-widespread-power-blackout-in-ukraine/; Yousra Khalil, "With the Internet Blackout in Sudan, Knowledge Is Power," The Washington Institute, June 25, 2019, https://www.washingtoninstitute.org/policy-analysis/view/with-the-internet-blackout-in-sudan-knowledge-is-power; Niha Masih, "'I'm Just Helpless': Concern about Kashmir Mounts as Communication Blackout Continues," *The Washington Post*, August 6, 2019, sec. Asia & Pacific, https://www.washingtonpost.com/world/internet-mobile-blackout-shuts-down-communication-with-kashmir/2019/08/06/346d5150-b7c4-11e9-8e83-4e6687e99814_story.html.
61. Ian Langford, "Accelerated Warfare," February 27, 2019, https://www.army.gov.au/accelerated-warfare-0.
62. Bryan Sparling, "Information Theory as a Foundation for Military Operations in the 21st Century" (School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, 2002), 51, https://apps.dtic.mil/dtic/tr/fulltext/u2/a403845.pdf.
63. Niall McCarthy, "The Institutions Americans Trust Most And Least In 2018," Forbes, June 29, 2018, https://www.forbes.com/sites/niallmccarthy/2018/06/29/the-institutions-americans-trust-most-and-least-in-2018-infographic/.
64. Rogers, "158. In the Cognitive War – The Weapon Is You!"