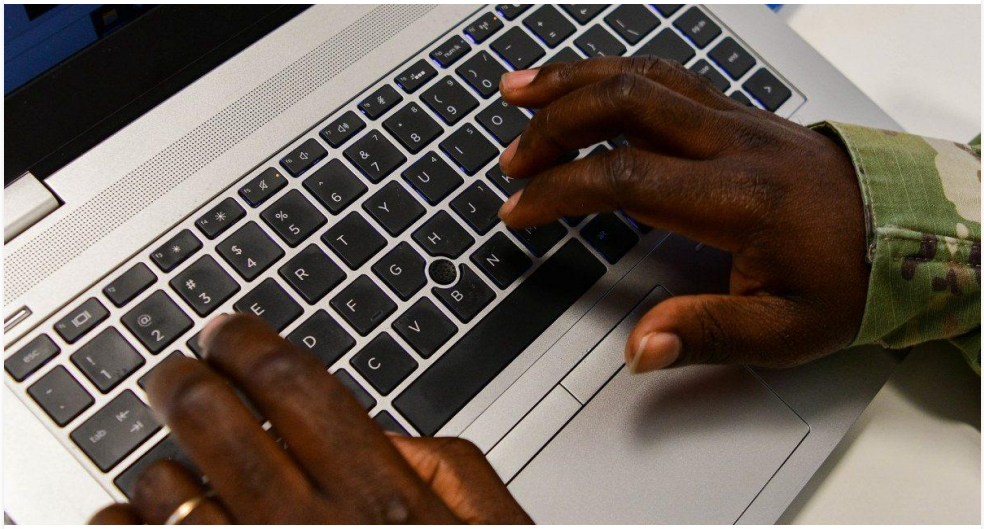
THE DEVIL IS IN THE DATA: PUBLICLY AVAILABLE INFORMATION AND THE RISKS TO FORCE PROTECTION AND READINESS

Joe Littell, Maggie Smith and Nick Starck | 09.20.22



In the early 2010s, mass protests and riots ripped through the Middle East and North Africa as the Arab Spring gathered support. Longtime authoritarians like Zine El Abidine Ben Ali of Tunisia, Hosni Mubarak of Egypt, Muammar Gaddafi of Libya, and Bashar al-Assad of Syria all struggled to contain the groundswell after

FOLLOW US

FACEBOOK

YOUTUBE

TWITTER

DISCLAIMER

The articles and other content which appear on the Modern War Institute website are unofficial expressions of opinion. The views expressed are those of the authors, and do not reflect the official position of the United States Military Academy, Department of the Army, or

decades of rule. The rest of the world watched the human rights atrocities broadcast live on social media directly from those living through it instead of from traditional media institutions or foreign correspondents. The ubiquity of cellular phones and social media had democratized media production and the world had a front-row seat to revolution and upheaval.

The shift in information sharing, from formal media to informal social media, was accompanied by a shift in who could *act* on that information. Fearless netizens began collecting images from Twitter and videos from YouTube, and comparing them with Google Street View and other publicly available reverse image search tools. People like Eliot Higgins, founder of open-source investigation and journalism outfit Bellingcat, cut their teeth on the media coming out of the Arab Spring and the bloody civil wars that followed. Most efforts were focused on doing good, and an entire human rights cottage industry sprung up around the new data sources and the analytic groups documenting violence as it happened all over the world. Many believed that we were finally seeing the promised societal benefits of innovative technologies and that the near-constant data collection and advanced analytic techniques, like artificial intelligence and machine-learning algorithms, would really change the world.

However, as with all technology, there is also a dark side to the big data explosion that poses significant risks to privacy and national security. The deliberate corporate collection of personal data, often referred to as the modern surveillance economy, has a singular goal—to shape consumer behavior. Put more bluntly, producers want consumers to buy more, and big data allows corporations to know what individuals like and what makes them click "purchase." But consumer data is not just available to corporate entities, in fact, anyone with the right amount of money can buy it in droves—nation-state adversaries can purchase data pools of publicly available information (PAI) about US consumers, their likes and dislikes, for analysis and influence, which is something that private marketing firms and authoritarian

Department of Defense.

The Modern War Institute does not screen articles to fit a particular editorial agenda, nor endorse or advocate material that is published. Rather, the Modern War Institute provides a forum for professionals to share opinions and cultivate ideas. Comments will be moderated before posting to ensure logical, professional, and courteous application to article content.

MOST POPULAR POSTS

Underground Nightmare: Hamas Tunnels and the Wicked Problem Facing the IDF

The Five Reasons Wars Happen

What Can the IDF Do about Hamas

regimes have been quick to exploit, and democratic governments have been slow to prevent.

The United States is still struggling to understand the national security risk posed by publicly available information. The 2018 Joint Concept for Operating in the Information Environment took steps to describe the information environment as consisting of three dimensions: the data-centric information dimension, the human-centric cognitive dimension, and the real-world physical dimension. Further, in 2022, the amended National Defense Authorization Act directed elements of DoD to *assess* the challenges of operating in the presence of "ubiquitous technical surveillance." Efforts to respond to these challenges are ongoing—among the notable endeavors are the Army's Information Advantage concept and the recent release of the Marine Corps Doctrinal Publication 8, *Information*. However, in the case of the Army's Information Advantage concept, the operationally focused efforts are overly narrow and fail to adequately address the scope of the challenges.

What DoD must acknowledge first is the fundamental source of risk to the US military from the information environment, namely the vast amounts of data collected and sold on US service members. And our adversaries can (and do) use the commercial data economy to target US service members and their families, and to pollute the information environment to diminish operational effectiveness. To adequately respond to this concerning shift in the operational environment, it is necessary to understand the categories of risk created by the collection of US service member data to help prioritize risk decisions and to improve the military's technical understanding of how the surveillance economy works. To frame the problem, we need to begin conceiving of actions in the data-centric information dimension as *creating* risk in the cognitive and physical dimensions of the information environment.

Cognitive Dimension Risks

Tunnels?

UPCOMING EVENTS

There are no upcoming events.

ANNOUNCEMENTS

Announcing the Modern War Institute...

Essay Contest Call for Submissions: Solving...

Call for Applications: MWI's 2023–24...

Join Us This Friday for a Livestream with...

The cognitive dimension of the information environment is defined by how humans understand, react to, and interact with the world based on the information they are exposed to. By extension, for the military, cognitive risks are any alteration to the perception and behavior of some number of individuals in a manner that will negatively impact a commander's ability to accomplish a mission or national priorities. Shaping perception and influencing behavior are two tasks that the modern surveillance economy is designed to facilitate and, when data on US persons is purchased, it can give enable adversaries to shape and influence how Americans think.

Like traditional operational risks, cognitive risks result from both adversary and friendly actions, and can manifest both internally and externally to an organization. Adversaries can use surveillance technologies to efficiently target key audiences, like service members, government employees, or even their families with mis- and disinformation. Friendly actions (and inactions) can also create cognitive risks, by eroding trust in the government and military, shaping fundamental behaviors like volunteering to enlist, and creating fodder for adversary information operations. Adversary operations may also target key military support constituencies and create cognitive risks to military operations, recruitment, and retention. For example, both Russia and Ukraine have leveraged these technologies during their ongoing conflict, creating cognitive risks from Russians calling and texting Ukrainian soldiers on the front lines to Ukrainians calling the mothers of Russian soldiers captured during the conflict. However, importantly—and critically for the US military—cognitive risks are *not* constrained to periods of armed conflict or deployment, and in many cases are more prevalent and impactful during normal garrison operations and are often external to any conflict.

Actualized examples of cognitive risks are numerous, and within the US population, they include mobilizing protestors, inflaming opinions on both sides of contentious social issues, and deepening issue divergence

among ideologically opposed groups. These examples show how surveillance technologies generate cognitive risk and may present a real threat during competition and crisis. Cognitive risks—with even the most tenuous connection to "traditional" Army missions—can pose some of the most serious risks to the force given their ability to fester and grow over time, erode trust, and disrupt cohesion within a unit and among key support constituencies. Ignoring or dismissing cognitive risks as falling outside of the Army's mandate or claiming that cognitive risks are an individual's responsibility is obtuse and potentially catastrophic to our ability to operate on the modern battlefield.

Protecting any population against cognitive risks is a delicate balance—particularly in a democracy. In the United States, First Amendment protections and an individual's freedom to access information are two characteristics of our democracy that malign actors regularly exploit and abuse to gain access to US service members' cognition. But by recognizing that cognitive risks exist and that they have the potential to impact mission success, we also create opportunities to act to thoughtfully detect, assess, and make risk decisions to drive mitigation efforts without having to consider the politics of the content being consumed. And effective risk categorization enables a better understanding of the threats to the force and will allow commanders to balance the informational freedoms we value with the need to defend the cognitive dimension.

Physical Dimension Risks

The most direct and obvious personal data risks to military forces occur in the physical world. Namely, publicly available information can be—and is—used for kinetic targeting. US government officials and service members, both at home and abroad, generate a lot of PAI as they go about their daily routines, revealing location data, travel data, purchasing data, and more. The concern for the military is how that personal data can be used to target individuals for kinetic strikes on the battlefield. The

ongoing conflict in Ukraine is an example of how PAI can be used to identify unsecure cell phones and enable location triangulation for kinetic attacks on conventional forces—in fact, at least one PAI-enabled kinetic strike has led to the death of a Russian general officer and Russia also leveraged PAI against Ukraine from 2014 to 2016.

However, the physical risk from PAI is not limited to location data. Imagery, from social media and official state sources, for example, can be compared to the robust database of landscapes found in programs like Google Earth, to pinpoint operationally relevant locations —a technique that led to the loss of a Russian naval vessel. The US military has also used similar targeting practices to direct drone strikes against ISIS targets using selfies and social media. Within DoD, therefore, commanders intuitively understand the seriousness of the tasks conducted to obfuscate their formations in time and space and the danger posed by inadvertent exposure. But increasingly, risks are coming from obscure places—like the 2018 example of how the exercise app Strava allowed for the identification of sensitive military locations through its Strava Heat Map feature. DoD responded with a new policy—nine months after the risk was identified—that banned the use of geolocation app features in deployed settings.

DoD's response to the Strava incident has since expanded to other technologies, including the Army's outright ban on cellphones for deploying troops, citing operational security and cybersecurity concerns. And even though the general awareness of physical risks created by data is growing (and is a good thing), an outright ban on certain technologies is not a sustainable risk mitigation strategy. The prohibition of personal devices is simultaneously too narrow and too broad and fails to strike an appropriate balance between necessary modernization and operational security. By focusing on conflict zones and deployed settings, DoD misses the physical risks those devices and their resulting PAI generate. And by banning devices and apps, DoD is inadvertently generating physical risks because typical patterns of life are suddenly

disrupted when those devices and apps go dark—the absence of digital data and signatures is also observable and could direct adversary attention to units and personnel heading overseas or conducting field training exercises. A more deliberate approach to assessing the risks in open-source data, and how actions in the information environment create signals for adversaries, is needed to achieve sustainable and substantive mitigation strategies.

The commercialization of personal data and the practices of commercial data brokers have enabled companies and our adversaries to accumulate vast amounts of knowledge on US persons, included our service members. Without fully understanding how these data systems impact military operational effectiveness, the United States sets itself at a strategic disadvantage. Understanding the vulnerabilities created by the commercial surveillance economy and identifying the associated risks is necessary for commanders to make informed risk decisions. While the wholesale removal of risk is not possible, a careful examination of risk can shape policy, open pathways for technical mitigation strategies, and define best data hygiene practices.

DoD's role in this effort should focus on gaining and maintaining operational security, which demands a layered approach that prescribes taking measured action at each echelon—individual, unit, and institutional—and prioritizing actions through a deliberate assessment of the operational risk. Importantly, any strategy must include individual education, institutional investment, and the implementation of privacy-preserving technologies. These efforts should mirror the approach taken toward cybersecurity, where DoD has acted to both secure its own networks and invested in initiatives like the Home Use Program to make security (or in this case, privacy) more accessible to its service members. Ultimately, without a layered approach to addressing the risks

generated by publicly available information and the surveillance economy, DoD will fail to protect its most valuable asset—its people—and will not be prepared to fight on the modern battlefield.

Major Joe Littell is a US Army psychological operations officer and research scientist at the Army Cyber Institute at the United States Military Academy.

Captain Maggie Smith, PhD, is a US Army cyber officer currently assigned to the Army Cyber Institute at the United States Military Academy where she is a scientific researcher, an assistant professor in the Department of Social Sciences, and an affiliated faculty of the Modern War Institute. She is also the coeditor of this series and director of the Competition in Cyberspace Project.

Major Nick Starck is a US Army cyber officer currently assigned as a research scientist at the Army Cyber Institute. His research focuses on information warfare and data privacy.

Image credit: Senior Airman Brooke Moeder, US Air Force