Finding the Enemy on the Data-Swept Battlefield of 2035

Capt. T. S. Allen, U.S. Army

In order to find the enemy today, armed forces point information collection assets, which may identify anything from a visual signature to a unique radio frequency, in the direction they think the enemy is until they find the enemy's location. This model is outdated because cyberspace's growth into a global control network that connects devices has created a new, data-swept battlefield, covered by billions of networked devices that are constantly sharing information and can be exploited to find the enemy more efficiently.[1]

By 2035, armed forces on the data-swept battlefield will typically find the enemy by exploiting data in cyberspace and in the broader information environment rather than by monitoring enemy forces directly with their own information collection assets.[2] Put more plainly, the enemy is going to broadcast where it is, or third parties are going to broadcast where the enemy is, as often as armed forces are going to point a camera or antenna at the enemy to find it. Armed forces will constantly query a wide variety of databases of both publicly available and sensitively acquired cyberspace information for indicators of where the enemy is located. Rather than visually or electronically scan for the enemy, the most efficient armed forces will "Google" the enemy using intelligence tools that exploit cyberspace.

On the data-swept battlefield, the armed force best postured to leverage cyberspace to find the enemy will have a significant advantage. The U.S. Army needs to break and remake its tactical intelligence model in order to prepare to win in these conditions.

Capt. T. S. Allen, U.S. Army, is a military intelligence officer serving in the Asymmetric Warfare Group at Fort George G. Meade, Maryland. He has previously served in Afghanistan and Korea, and he is qualified to plan cyberspace and information operations. Allen holds a BS in political science and military history from the U.S. Military Academy at West Point and an MA in war studies from King's College London.

Finding Targets on the Battlefield of 2035

The transformation of tactical intelligence to become cyberspace-centric is already underway.[3] The United States' enemies have been targeting its forces based on social media posts after operational security lapses since at least 2007.[4] For its part, the U.S. Armed Forces have bombed terrorists who made the mistake of posting selfies that revealed their locations.[5] As the number of networked devices and the frequency with which people use them to intentionally or unintentionally broadcast information continues to increase, the utility of existing cyber data streams to identify the location of anything, whether a consumer or an armored fighting vehicle, will also continue to increase.[6] Eventually, cyberspace and the broader information environment will

The digital viewer application, or DVA, provides the Army with a software-based video switching solution and allows command post personnel to connect to the local area network to share all or part of their display with other individuals or on the larger command post display system. (Photo simulation courtesy of the U.S. Army)

almost certainly become the United States' main source of intelligence, including tactical intelligence about the location and disposition of enemy forces. While U.S. forces will still use traditional information collection assets to pinpoint the locations of enemy units and fix them, they will also increasingly rely on cyberspace information to determine where to aim those sensors in the first place. After all, there is no need to patrol an entire province hunting for an enemy tank column when someone tweets a selfie that shows the tanks in the background or when a tank column's movement along a highway causes a massive disruption in well-established civilian traffic patterns that can be easily identified in traffic data collected by cell phone navigation applications.

To date, the transformation of tactical intelligence by cyberspace has been most apparent in the discipline of open-source intelligence (OSINT). Since the birth of the "Social Web," also known as "Web 2.0," in the late 1990s, user-generated content on social media has been central to internet culture. Additionally, smartphones, which allow users to upload content from almost anywhere and to rapidly capture and disseminate images, have come to function as billions of networked information collection devices that publicly share many of their findings on social media. The result has been the proliferation of publicly available information of operational and intelligence value.[7] Even civilian organizations now have the ability to conduct intelligence assessments with a high degree of accuracy using this data. In one notable example, the Atlantic Council and Vice News were able to identify individual Russian soldiers covertly fighting in Ukraine based

Soldiers configure the tactical computing environment extend mode, which pieces together various points on a digital map to create one, large map-view similar to what is available in larger command posts. This technology can help soldiers collaborate and increases situational awareness across a formation by sharing a near real-time common operating picture of the "data-swept battlefield." (Photo courtesy of the U.S. Army)

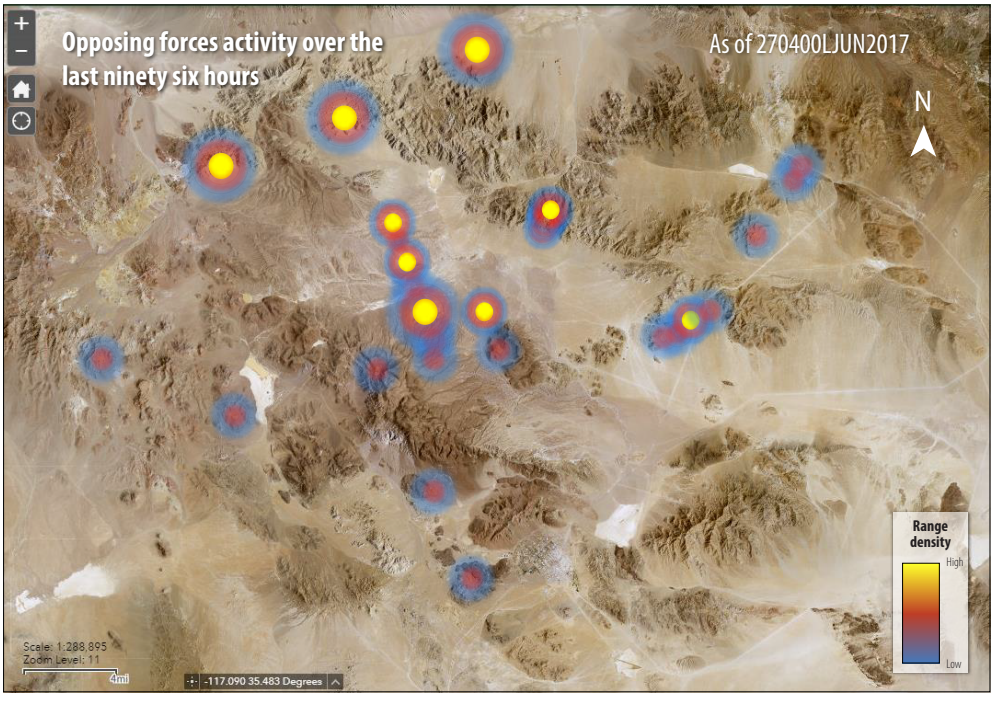
on their social media activity in 2014.[8] Similarly, the investigative journalism website Bellingcat has been able to consistently deliver high-quality intelligence assessments based almost exclusively on what it calls "open-source intelligence" derived from social media. As civilian open-source analyst Cameron Colquhoun notes, "Amongst the billions of posts, uploads, shares and likes, individuals again and again betray their interests to painstaking observers."[9]

Nonetheless, based on my experience as an intelligence officer, OSINT has not become the main source of tactical intelligence. For one thing, it relies heavily on users, who are not controlled or vetted, freely sharing information on events of interest. Users have strong reasons not to monitor military forces, which are armed and dangerous. Even when users do so, they rarely do so persistently, and since tactical intelligence is rapidly perishable, OSINT is only rarely useful for finding the enemy at the tactical level.

Between now and 2035, cyberspace will complete another massive transformation like that previously seen with smartphones and social media, and the effects of the next transformation on tactical intelligence will be even more significant. The new transformation is driven by the rise of the "Internet of Things" (IoT). Cyberspace has already transitioned from a global communication network that connects people to a global control network that connects devices, as Laura DeNardis argues in *The Internet in Everything: Freedom and Security in a Network World.*[10] Devices are now responsible for more cyberspace activity than people, and cyberspace is used to control everything from thermostats in private homes to industrial control systems in factories. Because the IoT is largely automated, the users whose uncontrollable behavior limited the tactical utility of OSINT derived from Web 2.0 are now irrelevant. "If humans suddenly vanished from the earth," DeNardis writes, "the digital world would still

vibrantly hum."[11] The Army's cyberspace doctrine will likely change to reflect this. While the current doctrinal cyberspace characteristics emphasize that cyberspace is "socially enabling," the Army already has ample reason to also characterize cyberspace as "largely automated."[12]

The IoT presents exciting tactical intelligence opportunities. If intelligence and cyber operations are integrated effectively, the IoT could become an unprecedented goldmine of intelligence, giving intelligence collectors access to a countless number of sensors to find the enemy. Whereas during the Vietnam War, the United States tried to monitor wide areas by airdropping thousands of sensors into the jungle, in the future, similar objectives could be accomplished by exploiting civilian sensors that are already in use.[13] Devices such as home security cameras have information of intelligence value if they are pointed at the right location; given how common they have become, it is certain that some IoT sensors will be pointing at areas of interest at least some of the time. Moreover, IoT devices are infamously insecure, as hackers regularly demonstrate.[14] As of early 2020, 98 percent of IoT traffic was unencrypted, making it exceptionally easy to exploit.[15] The major significant disadvantages of exploiting IoT sensors are that they cannot be technically controlled and are vulnerable to deception and manipulation, but these weaknesses will be checked by the sheer scale of data available, which can be used to add ever more information with which to make assessments.



(Figure by Capt. Gerald Prater, U.S. Army. Orthoimagery map courtesy of the U.S. Geological Survey's The National Map)

Heat Map of the Location of Opposing Forces at the National Training Center in 2017

Two innovative lieutenants produced the map by using social media location data, which could have been produced from anywhere in the world, requiring no special intelligence equipment.

As the IoT develops, one significant emerging common practice is that most vehicles broadcast data about their locations. Although the Army will not primarily find the enemy inside the United States, U.S. cyber practices frequently proliferate worldwide, so they are an important leading indicator. In the United States today, all aircraft already emit their locations through a system called automatic dependent surveillance–broadcast (ADS-B), and most ships do the same through the automatic identification system. The U.S. Department of Transportation also advocates the employment of vehicle-to-vehicle safety communications systems for most private automobiles that would broadcast location data.[16] By 2035, systems such as ADS-B, the automatic identification system, and vehicle-to-vehicle will almost certainly proliferate worldwide. While these systems are designed to ensure security and a modicum of privacy, since they still share location data, in practice they will make it possible for any appropriately equipped automated device to easily monitor all vehicular movement. Moreover, if ADS-B is any guide, fixed sensors that monitor movement activity and

automatically share it in cyberspace are likely to become common to satisfy public demand for data about traffic. As the Government Accountability Office found in a 2018 assessment of ADS-B, these systems pose grave risks to the operational security of military forces, including our own, because they could require us to broadcast the locations of sensitive military activities.[17]

There is also an emerging but contested norm that human beings share data about their locations in cyberspace via their phones and wearable IoT devices. The Department of Defense received a stunning reminder of this in 2018 when Strava, a fitness device company, published a heat map based on users that highlighted running routes on military bases around the world.[18] It received another in 2019, when the *New York Times* reported it used cell phone location data to track the movements of a senior defense official.[19] The sharing of location data is likely to continue because, as Shoshanna Zuboff argues, corporations profit from exploiting user location data, and most users are willing to provide it. While many people are uncomfortable with the notion that they are being tracked individually, they often have little objection with the sharing of data that is labeled "aggregated" or "anonymous."[20] The COVID-19 pandemic has brought significantly more public attention to cell phone location trackers.[21] During the pandemic, Google used its database of smartphone user locations to provide detailed reports to public health officials on patterns of life around the world and publicly released them.[22] In a more germane use case, a private sector geospatial analytics company reported that Russian arms factories were slowing production by leveraging similar data to see how many factory employees were reporting to work during the pandemic.[23] Interestingly, only five days later, the Russian government banned military personnel from carrying smartphones that track user location.[24]

A 2018 heat map showing the movement of soldiers based on location data collected from the Strava fitness application at Bagram Air Base in Afghanistan. (Screenshot courtesy of Strava Labs)

By 2035, then, we will live in a world where most movement generates a cyberspace signature. Vehicular movement will be easy to track, and at the very least, broad trends in individual human movement will be visible. Chances are no one will install tracking systems on military vehicles but that will not reduce the intelligence value of this massive data source. Military forces will maneuver across a data-swept battlefield, where every "hidden" action they take sparks an easily monitored reaction. Even if they emit nothing, they will be indirectly visible in cyberspace when they disrupt normal patterns of life, when they cause traffic jams by driving down highways, when people post information about their activities on social media, and when they come into the field of view of exploitable IoT devices such as security cameras. In many cases, analysts will be able to find the enemy by identifying disruptions in normal patterns of life showing *atypical inactivity* in a given area. I term this "negative intelligence," akin to the meaningful emptiness of "negative space" in visual media. While military organizations may not necessarily deliver lethal fires on targets identified only in cyberspace, cyberspace will provide the intelligence base layer in which intelligence forces find the enemy. Traditional information collection assets will still play an important role, but they will focus on fixing enemy forces that were found in cyberspace.

The force that is best prepared to access the wide variety of information of intelligence value in cyberspace will have a decisive advantage over another force that limits itself to fewer, technically controlled information collection assets that will only be able to collect an exponentially smaller amount of data.

This is Not the Battlefield You Are Looking For

The data-swept battlefield of 2035 presents exciting intelligence opportunities, but it also presents daunting challenges for the U.S. Army. In order to achieve a decisive advantage, the Army must make fundamental changes to its tactical intelligence model, even beyond the changes outlined in *The U.S. Army in Multi-Domain Operations 2028*, which describes its future vision but does not mention the IoT.[25] These changes are imperative because if they are not implemented, the Army could find itself suffering from chronic information overload, incapable of conducting mission command, and fighting in future wars without many of its historic advantages.

First and most importantly, the Army must prepare to exploit cyberspace information at centralized, highly automated intelligence centers focused on supporting tactical decision-making that will identify information of tactical value, process it, exploit it, and disseminate it to tactical formations for action. Historically, it made sense for the Army to expect commanders to find many of their own targets because they could do so with close-access information collection assets in their formations. The data-swept battlefield will change this as most IoT devices are designed to be networked and share information globally, making close access less important. IoT devices share data through a cyberspace that will be increasingly "centralized," with massive corporations such as TenCent in China and Yandex in Russia controlling an unprecedented share of all data.[26]

While the centralization of the internet will require the centralization of intelligence collection,

Spc. Nathaniel Ortiz, Expeditionary Cyber Electromagnetic Activities (CEMA) Team, 781st Military Intelligence Battalion, conducts cyberspace operations 9 May 2017 at the National Training Center, Fort Irwin, California. More recently, the 915th Cyberspace Warfare Support Battalion activated on 1 January 2019 is the first scalable organic expeditionary capability to meet the Army's current and projected tactical CEMA requirements. (Photo by Bill Roche, U.S. Army Cyber Command)

Members of the 6th Special Operations Squadron use a tablet to upload coordinates 17 December 2019 during an exercise showcasing the capabilities of the advanced battle management system (ABMS) at Duke Field, Florida. During the first demonstration of the ABMS, operators across the Air Force, Army, Navy, and industry tested multiple real-time data-sharing tools and technology in a homeland defense-based scenario enacted by U.S. Northern Command and enabled by Air Force senior leaders. (Photo by Tech. Sgt. Joshua J. Garcia, U.S. Air Force)

Army decision-making must remain widely distributed to maintain tactical flexibility. As a result, the new intelligence centers will have to get better at disseminating what they know down to the tactical level, primarily through existing theater military intelligence brigades attached to field armies, to augment close-access sensors.[27] Because of the massive amount of data that must be processed, artificial intelligence and machine learning will become key to processing and exploitation. Intelligence collection managers on the data-swept battlefield of 2035 will be modifying algorithms to answer their information requirements. Otherwise, they will almost certainly face information overload—and intelligence failure.[28] Echeloning intelligence capabilities and taking advantage of economies of scale at higher echelons will help avoid creating information overload at lower echelons.

Second, in order to properly exploit the data-swept battlefield, the Army must break down silos between the cyber and intelligence communities. Exquisite capabilities that are currently used for cyberspace intelligence, surveillance, and reconnaissance will have to be repurposed to answer intelligence requirements for maneuver commanders.[29] Rather than simply attaining situational awareness *of* cyberspace as current doctrine states, cyber forces will have to enable intelligence forces by attaining situational awareness of *all domains through cyberspace*.[30] This will require intelligence and cyber forces to share information seamlessly in support of tactical commanders, as part of "convergence," the Army's goal of delivering the "rapid and continuous integration of all domains across time, space and capabilities to overmatch the enemy."[31]

Third, the Army needs to prepare for its own tactical-level actions to be visible in cyberspace. Every new intelligence opportunity is also a potential operational security threat. The Army's operations security model runs the risk of becoming outdated; it remains focused on emissions control, but by 2035 it will have

to control or obfuscate the emissions of the civilian devices that will constantly monitor Army forces on the data-swept battlefield. Because controlling all of these devices is impossible, obfuscation and deception will become more important, even at tactical echelons.[32] Army operations security planners must also increasingly think "two steps ahead" and prepare to fight and win even after their activities are disclosed to the entire world. The Army will have to push enhanced obfuscation and deception capabilities down to lower echelons than ever before, far below the corps level, which is currently the lowest echelon it envisions deploying military deception capabilities.[33] On the data-swept battlefield, even small tactical units will need the cyber equivalent of fog machines.

Fourth, the Army must take deliberate steps to preserve mission command when technology enables micromanagement. As Marshall McLuhan wrote in 1964, "In the long run, a medium's content matters less than the medium itself in influencing how we think and act."[34] Advanced command-and-control technology almost always undermines mission command because it makes micromanagement easy. When the telegraph was first used in military operations in the Crimean War in 1855, the French commanding general immediately found that "the paralyzing end of an electric wire" made it easier for his leaders in Paris to give him orders without adequate information and harder for him to respond to situations on the ground as they developed.[35] In the future, when a battalion commander in an operations center has more information on where an enemy force is located than a platoon leader in contact with that same enemy force, the battalion commander will be tempted to micromanage the platoon leader. However, the flexibility of mission command continues to give American forces a decisive advantage.[36] As a result, we must take careful steps to preserve human-centric mission command within our forces as technology advances.

Fifth, the Army needs to be sensitive to the civil-military-technical concerns that will arise on the data-swept battlefield. The "data" is almost all proprietary and controlled by private industry. While private companies with access to this data participate in a thriving market for data on the activities of private citizens around the world, data brokers may be hesitant to share information with armed forces that will use it for military or intelligence purposes. Relationships with these data brokers will be more important than ever before (and also likely more tense). Given privacy rights and other legitimate data protection concerns, the exploitation of data about foreign targets that is owned by businesses located in the United States or allied nations will continue to be a thorny issue. Additionally, the exploitation of civilian devices will likely raise novel law-of-war issues.

For those interested in reading more about cyber defense, *Military Review* recommends the Spring 2020 edition of *The Cyber Defense Review* (*CDR*). *The CDR* journal is a scholarly effort from the Army Cyber Institute at West Point. *The CDR* generates an intellectual multidisciplinary dialogue through thought-provoking scholarly articles and essays on the strategic, operational, and tactical aspects of the cyber domain. *The CDR* breaks down barriers and fosters innovative solutions to global cybersecurity challenges. *The CDR* compiles perspectives from preeminent thinkers across the government, industry, and academia regarding potential challenges, impacts, and initiatives for consideration as we solve over-the-horizon problems for the Army and the Nation. To view the Spring 2020 edition of *The CDR*, visit https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Summer%202000/CDR%20V5N2%20Summer%202020-r8-1.pdf.

Finally, the Army must recognize that there is a real chance that its adversaries will have an advantage in the cyberspace tactical intelligence fight. Many of the material advantages afforded by the Army's exquisite legacy information collection assets will be less important on the data-swept battlefield, and it will have to develop new nonmateriel advantages. Just because the United States has led the information revolution does not mean the U.S. Army is best postured to dominate future battlefields.[37]

Many of the United States' adversaries are postured to out-innovate it. As David Kilcullen demonstrates in his 2020 book *The Dragons and the Snakes: How the Rest Learned to Fight the West*, U.S. adversaries have outpaced it in part by exploiting systems the United States originally built and later made available for civilian use, such as the internet and GPS.[38] Because many cyberspace activities have relatively low resource requirements, and above all, require adaptation to an ever-changing cyber environment, nimble, unrestrained nonstate actors have an advantage over large state bureaucracies such as the Army.[39] There are promising signs that the Army can innovate too, such as the examples of soldiers who figured out how to find enemy forces by exploiting social applications like Tinder and Snapchat that reveal locational data.[40] While bottom-up innovators cannot build the centralized, scalable solutions the Army needs, the Army must do more to enable the innovative hackers in its ranks.[41]

Conclusion

The data that will sweep over the battlefield of 2035 and fundamentally change tactical intelligence is already slowly accumulating in databases around the world. On future battlefields, traditional information collection assets will still play a critical role in allowing armed forces to fix enemy forces, but because of the proliferation of networked devices that automatically broadcast staggering amounts of data in the IoT, the *find* phase of the targeting process will be cyber-centric. In order to maintain its advantages on future battlefields, the Army must enhance its ability to find the enemy is cyberspace in support of tactical intelligence, starting now. ■

Notes

1. For a discussion of the fire-swept battlefield, see Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 30. The term "data-swept battlefield" is the author's and is original to this article. It is a reference to the "fire-swept battlefield," which characterizes contemporary ground combat.

2. *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, as of June 2020), 55 and 104, accessed 15 September 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727. "Cyberspace" is defined as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The "information environment" is defined as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."

3. T. S. Allen and Robert A. Heber Jr., "Where Posting Selfies on Facebook Can Get You Killed," *Wall Street Journal* (website), 26 July 2018, accessed 15 September 2020, https://www.wsj.com/articles/where-posting-selfies-on-facebook-can-get-you-killed-1532642302.

4. "Insurgents Used Cell Phone Geotags to Destroy AH-64s in Iraq," Military.com, 15 March 2012, accessed 15 September 2020, https://www.military.com/defensetech/2012/03/15/insurgents-used-cell-phone-geotags-to-destroy-ah-64s-in-iraq.

5. Walbert Castillo, "Air Force Intel Uses ISIS 'Moron' Post to Track Fighters," CNN, 5 June 2015, accessed 15 September 2020, https://www.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html?mod=article_inline.

6. Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," *New York Times* (website), 19 December 2019, accessed 15 September 2020, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

7. Heather J. Williams and Ilana Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise" (Santa Monica, CA: RAND Corporation, 2018), accessed 15 September 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

8. "Selfie Soldiers: Russia Checks in to Ukraine," VICE News, 16 June 2015, accessed 15 September 2020, https://www.vice.com/en_us/article/bjk9na/selfie-soldiers-russia-checks-in-to-ukraine.

9. Cameron Colquhoun, "A Brief History of Open Source Intelligence," Bellingcat, 14 July 2016, accessed 15 September 2020, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

10. Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, CT: Yale University Press, 2020).

11. Ibid., 3.

12. Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office

[GPO], 11 April 2017), para. 1-64, accessed 15 September 2020, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002097.

13. Matt Novak, "How the Vietnam War Brought High-Tech Border Surveillance to America," Gizmodo, 24 September 2015, accessed 15 September 2020, https://paleofuture.gizmodo.com/how-the-vietnam-war-brought-high-tech-border-surveillan-1694647526.

14. Joseph Cox and Samantha Cole, "How Hackers Are Breaking into Ring Cameras," VICE News, 11 December 2019, accessed 15 September 2020, https://www.vice.com/en_us/article/3a88k5/how-hackers-are-breaking-into-ring-cameras.

15. Unit 42, "2020 Unit 42 IoT Threat Report," Palo Alto Networks, 10 March 2020, accessed 15 September 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

16. T. S. Allen, "Open-Source Intelligence: A Double-Edged Sword," *Proceedings* 144, no. 8 (August 2018), accessed 15 September 2020, https://www.usni.org/magazines/proceedings/2018/august/open-source-intelligence-double-edged-sword.

17. U.S. Government Accountability Office (GAO), *Homeland Defense: Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft* (Washington, DC: U.S. GAO, January 2018), accessed 15 September 2020, https://www.gao.gov/assets/690/689478.pdf.

18. Patrick Tucker, "Strava's Just the Start: The US Military's Losing War Against Data Leakage," Defense One, 31 January 2018, accessed 15 September 2020, https://www.defenseone.com/technology/2018/01/stravas-just-start-us-militarys-losing-war-against-data-leakage/145632/.

19. Thompson and Warzel, "Twelve Million Phones, One Dataset, Zero Privacy."

20. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Hachette Book Group, 2019), 242–45.

21. Sara Morrison, "The Hidden Trackers in Your Phone, Explained," Vox, 8 July 2020, accessed 15 September 2020, https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

22. "COVID-19 Community Mobility Reports," Google, last updated 13 September 2020, accessed 15 September 2020, https://www.google.com/covid19/mobility/.

23. Patrick Tucker, "Russian Arms Production Slowed by Coronavirus, Analysts Find," Defense One, 1 May 2020, accessed 15 September 2020, https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/.

24. "Putin Bans Armed Forces Members from Carrying Electronic Devices, Gadgets," Radio Free Europe/Radio Liberty, 7 May 2020, accessed 15 September 2020, https://www.rferl.org/a/putin-bans-armed-forces-members-from-carrying-electronic-devices-gadgets/30598888.html.

25. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), accessed 15 September 2020, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

26. Prem Tummalacherla, "The Top 3 Issues of the Centralized Internet," Medium, 14 June 2019, accessed 15 September 2020, https://medium.com/@IamPremt/the-top-3-issues-of-the-centralized-internet-1db59d5e495e.

27. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

28. Tom Lamont, "Can We Escape from Information Overload?," *The Economist* (website), 29 April 2020, accessed 15 September 2020, https://www.economist.com/1843/2020/04/29/can-we-escape-from-information-overload.

29. FM 3-12, *Cyberspace and Electronic Warfare Operations*, para. 1-41.

30. Ibid., para. 1-71.

31. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, iii.

32. Edward Geist and Marjory Blumenthal, "Military Deception: Ai's Killer App?," War on the Rocks, 23 October 2019, accessed 15 September 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

33. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 22.

34. Marshall McLuhan, quoted in Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), 3.

35. Gordon Wright, "Soldiers and Statesmen in 19th Century France," in *Soldiers and Statesmen: The Proceedings of the 4th Military History Symposium*, ed. Monte D. Wright and Lawrence J. Paszek (Washington, DC: Office of Air Force History, Headquarters USAF; and United States Air Force Academy, 1973), 28.

36. B. A. Friedman and Olivia A. Garard, "Technology-Enabled Mission Command," War on the Rocks, 9 April 2020, accessed 15 September 2020, https://warontherocks.com/2020/04/technology-enabled-mission-command-keeping-up-with-the-john-paul-joneses/.

37. Kenneth Pollack, "Society, Technology, and Future Warfare," American Enterprise Institute, 6 November 2019, accessed 15 September 2020, https://www.aei.org/research-products/report/society-technology-and-future-warfare/.

38. David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (New York: Oxford University Press, 2020), 38–65.

39. Stephen Rodriguez, "The Fox in the Henhouse: How Bureaucratic Processes Handicap US Military Supremacy and What to Do about It," Atlantic Council, 26 February 2020, accessed 15 September 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-fox-in-the-henhouse-how-bureaucratic-processes-handicap-us-military-supremacy-and-what-to-do-about-it/.

40. Curt Taylor, "It's Time for Cavalry to Get Serious about Cyber Reconnaissance," eArmor, Fall 2018, accessed 15 September 2020, https://www.benning.army.mil/Armor/eArmor/content/issues/2018/Fall/4Taylor18.pdf; Gina Harkins, "A Lance Corporal's Phone Selfie Got His Marine Unit 'Killed' at 29 Palms," Military News, 7 January 2020, accessed 15 September 2020, https://www.military.com/daily-news/2020/01/07/lance-corporals-phone-selfie-got-his-marine-unit-killed-29-palms.html.

41. James Long, "Shoot, Move, Communicate, and Innovate: Harnessing Innovative Capacity in the Ranks," Modern War Institute at West Point, 16 March 2020, accessed 15 September 2020, https://mwi.usma.edu/shoot-move-communicate-innovate-harnessing-innovative-capacity-ranks/.