THE CYBER DEFENSE REVIEW

A Military of Influencers

Author(s): Robert J. Ross and Josh Rutland

Source: *The Cyber Defense Review*, FALL 2022, Vol. 7, No. 4 (FALL 2022), pp. 213-226

Published by: Army Cyber Institute

Stable URL: https://www.jstor.org/stable/10.2307/48703301



# A Military of Influencers: The U.S. Army Social Media, and Winning Narrative Conflicts

Lieutenant Colonel Robert J. Ross, Ph.D.
Josh Rutland

## ABSTRACT

*In the interconnected era of the Internet, the military must confront the new face of an old threat: narrative conflict. Where states once maintained nearly absolute domestic control of the narratives surrounding their military engagements, social media have created a wide array of perspectives, arguments, and disinformation campaigns that constantly affect both the civilian and military populations. These campaigns encourage the questioning of state objectives and threaten the identity of the individual and the collective ontological identity of the society, making it more difficult for states to maintain momentum and support for their military endeavors. Without that support, military campaigns can collapse, regardless of the skill or preparedness of warfighters. This research explores three topics relevant to the U.S. Army in hopes of helping it better equip itself to succeed in narrative conflicts: the strategic impacts of commander's decisions on the battlefield, the need to control signals emissions, and the consequences of bulk internet data sales. It then concludes by providing brief policy suggestions for mitigating these issues.*

## INTRODUCTION

When the Gutenberg printing press emerged in the late 15th century, it rocked the foundations of societal order in Europe by establishing the first networked era.[1] The ensuing mass production of pamphlets made them accessible to the common person.[2] As the masses of common Europeans began to study religious texts for themselves, new perspectives emerged to challenge the church's


**Lieutenant Colonel Robert J. Ross** is the Strategic Initiatives Group Chief for the Commanding General of U.S. Army Cyber Command, Fort Gordon, GA. Lieutenant Colonel Ross advises the ARCYBER Commanding General on cybersecurity, information-age conflict, and information warfare strategy. He is a former assistant professor in the Electrical Engineering and Computer Science Department at the U.S. Military Academy at West Point, NY. He is a former Chief Research Scientist for the Army Cyber Institute, a position in which he served as the Information Warfare Team Lead. He has a B.S. degree in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Lieutenant Colonel Ross is a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare, 21st century conflict, and financial technology.

authority.[3] Ultimately, the increasingly rapid dissemination of information through advancing technology caused the questioning, undermining, and weakening of the authority of the Roman Catholic Church, which had dominated religious narratives in Europe for more than 1,000 years.

Technology has continued to grow in modern times, with mobile phones and the Internet creating a network of instantaneous communications much, much larger in scope than that of Gutenberg's printing press. The growing technology has amplified impacts on society, with conventional authorities facing unprecedented challenges to their leadership. The time has passed for state control over the information flow across and within its borders using traditional media methods, and official narratives that shaped public opinion in support of the state. Political and ideological dissonance quickly and ubiquitously pours across the borderless Internet from which the global audience drinks.[4] Blog posts, cell phone footage, podcasts, drone recordings, and myriad other content forms are deemed valid regardless of merit or origin.[5] Collectively, they form the new narratives consumed and further propagated by the masses on social media. The result is, once again, a questioning of conventional authority and the degradation of that authority's power at an unprecedented rate. The walls of Westphalia have fallen again.

These developments have troubling implications for contemporary warfighting scenarios, which require a motivated military and citizenry for victory. While traditional military conflict continues, as in the Russian invasion of Ukraine, and remains a critical component of warfare, the importance of narrative conflict has never been greater. The Internet, mobile phones, and social media offer an opportunity for states to infiltrate the minds of their adversaries' citizenry through

**Josh Rutland** is a graduate of Augusta University's Master in Intelligence and Security Studies program. He currently works as a researcher in the Augusta University Department of Emergency Medicine and will soon be employed by ARCYBER as an Information Technology Specialist. His research focuses on information warfare, cybersecurity, terrorism, and biosecurity. His work has appeared in such journals as *Politics and the Life Sciences, Politics & Policy, Behavioral Sciences of Terrorism and Political Aggression, Journal of Cyber Policy, and PLOS Global Public Health*.

widespread, tailored propaganda efforts. These efforts may be designed to facilitate a variety of outcomes, including diminished support for a war. Demoralization on such a wide scale threatens to "rob an army of its spirit and a commander of his courage," which Sun Tzu described as the key to victory, destroying an adversary's will to fight without so much as a single battle.[6] The Islamic State of Iraq and Syria's (ISIS) victory over the Iraqi Army at Mosul provides a potent example of the power of narrative: The 10,000 troops present in Mosul had mostly abandoned their posts out of fear spawned by ISIS terror campaigns that streamed across the Internet long before ISIS forces arrived in the city.[7] The result was an easy victory for ISIS forces. Though the Iraqi force was larger and better armed, its fear of ISIS ultimately ensured its defeat.[8] Even the US has fallen prey to the effects of narrative defeat during the wars in Vietnam, Iraq, and Afghanistan. Wars can be won or lost based on their surrounding narratives despite overwhelming tactical victory in every engagement using traditional military force.

This article argues that winning modern narrative conflicts will demand doctrinal change within the Army and other services in some key areas relevant to information operations, public affairs, psychological operations, and cyber space operations. The study focuses on three important issue areas: the strategic impacts of soldiers' decision-making, vulnerabilities related to signature management, and the threats posed by bulk data collection and sales conducted by third party social media platforms. To demonstrate this point, the article proceeds in two sections. First, we briefly analyze the three focal issue areas using existing literature that highlights their importance and details the security issues. Then, we provide relevant policy suggestions, based on modifications of former and existing Army doctrine generated from researching this topic.

## THE STRATEGIC CORPORAL

U.S. Marine General Charles Krulak conceptualized the strategic actions at the lowest tactical level in his 1999 essay titled "The Strategic Corporal." Krulak argued that "success or failure will rest, increasingly, with the rifleman and with his ability to make the *right* decision at the *right* time at the point of contact" with both the enemy and the local population.[9] In addition to the pressures of high stress environments where lives are at stake; the soldier in the field also bears the burden of overcoming two major obstacles: a general hostility and weariness on the part of the local population and the mutually perceived cultural divisions between one's own "ingroup" and the "outgroup" that inhibit communication and personal bonding.[10] While this places additional demand on warfighters, their ability to understand and adopt relevant customs and behaviors of the indigenous populations with which they interact will shape their own personal relationships within that society and the general disposition of that society toward other warfighters with whom they interact in the future.[11]

As such, the ability of Army warfighters also to function and be perceived as "cultural mediators" and community members when interacting with a foreign populace is a critical tool that must be maintained like any other piece of equipment in a soldier's toolkit.[12] This has led to calls for redesigned professional military education processes that highlight the importance of language training, cultural education, and "educational and experiential cross-fertilization between the military and other government agencies" or humanitarian organizations relevant to future operational fields.[13] Major Linda Liddy of the Australian Army also argues that the modern soldier will need to be academically savvy in topics such as "military law and leadership, military history, and current affairs and ethics" in order to prepare fully for their role as warfighters and influencers expected to carry out complex operations with military and humanitarian ambitions.[14]

The omnipresence of cell phones with cameras and Internet connectivity further ensures that tactical-level actions, positive or negative, will ripple across the societies with which they interact and extend beyond their immediate communities.[15] Strategic adversaries could coopt footage depicting cultural insensitivity, whether accidental or deliberate, to fuel terrorist recruitment[16] or turn large populations and Internet communities against the U.S. Army. This could diminish its security, morale, and chances of operational success.[17] Warfighters must do everything in their power to set themselves apart in the minds of those with whom they interact in operational theaters to establish mutual respect, cooperation, and beneficence.[18] A warfighter has a personal presence in the minds of those with whom they interact. This means that the warfighter ceases to be simply an American or a soldier to become a friend or community member, which can be critical in environments such as the Middle East where cultural and familial bonds mean far more than shared regional or territorial residency. In short, impressions and reputations are critical; they can make or break an operation tactically and narratively.[19] Warfighters will need to be able to shape their reputations in a positive way to ensure operational success.

## SIGNATURE MANAGEMENT VULNERABILITIES

Signature management vulnerabilities are those associated with the impacts on battlefield events or troop deployments of signals emitted and received from electronic devices.[20] While myriad strategic vulnerabilities exists with respect to signature management and narrative conflict, two significant threats stem from physical infrastructure and "digital exhaust,"[21] which is described by Harper Reed as "a constant trail of activities, behaviors, preferences, signatures, and connections" left behind by every digital device that is tied to both that device and its user.[22] Both have the potential to contribute to adversaries' interception of sensitive information regarding Army units, ultimately resulting in "the design and development of adversary systems, tactics, training, and force preparations capable of countering Army unit capabilities, activities, and intentions."[23] As such, new considerations must be accounted for to limit public knowledge of Army units and their deployments successfully.

Control of physical infrastructure means control over and access to any signals that pass through it.[24] Army units thus cannot be sure their communications are secured when operating in a foreign theater where critical infrastructure is built, owned, and operated by potentially adversarial forces.[25] As the world transitions to 5G technology, this becomes an even greater risk, as 5G infrastructure is being built primarily by China across parts of Asia, Africa, and Europe.[26] This gives China "access to the private data of billions of people" which may include "individuals' medical histories, spending habits, political views, personal details expressed on social media, physical location, financial situation" and much other data the state could adapt to "gain a commercial or technical advantage in data-driven markets, target key individuals for recruitment by intelligence operations, or compromise political figures."[27] Civilians are not the only potential target of this type of data collection. Anyone using the network is vulnerable.[28] As such, it is imperative that the Army anticipate this battlefield vulnerability and develop alternatives to using foreign infrastructure, such as establishing its own permanent infrastructure in contested regions of influence.[29]

While physical infrastructure poses a significant vulnerability, digital exhaust may represent the most significant threat associated with signature management. Digital exhaust refers to the impact on the virtual realm resulting from military movements and engagements.[30] Adversaries could use this information to determine troop movements before they are made public, putting warfighters in harm's way, risking operational failure, and presenting adversaries with an opportunity to humiliate or propagandize against their opponent. The Bellingcat Study, the Second Nagorno-Karabakh War, and recent events in Ukraine all represent examples of how dangerous digital exhaust can be in the wrong hands.

During the Bellingcat Study, a handful of amateur Internet sleuths crowdsourced information largely comprised of the Russian military's digital exhaust to provide decisive evidence that Russian forces had shot down Malaysian Airlines Flight MH17 in July 2014.[31] The Bellingcat

group, led by Eliot Higgins, used online videos and photographs to identify the specific Buk anti-aircraft missile that had shot down MH17.[32] It then collected a number of videos and photographs of the Buk that enabled it to plot successfully a timeline and geographic trail of its movements from Russia into Ukraine which proved Russia's culpability in MH17's destruction.[33] The discovery forced Russia into a losing battle with the Bellingcat group to control the narrative surrounding the MH17 incident that ultimately resulted in the Russian government's embarrassment.[34] The Bellingcat group harnessed the power of social media to expose a global power and its army.[35] Anyone with a vested interest, state-or civilian-sponsored, could employ Bellingcat's methods against any army, should that army fail to account for its troops' digital exhaust.

The Second Nagorno-Karabakh War between Armenia and Azerbaijan represents a more direct example of digital exhaust exploitation by one state against another.[36] Using Turkish Bayraktar TB2 drones and Israeli HAROP Loitering Munitions (LM) , Azerbaijani forces devastated the Russian-supported Armenian ground forces through the nearly exclusive use of unmanned strikes.[37] The cameras inside these drones captured live footage of the bombing and the destruction from the strikes, which was then broadcast to both sides by the Azerbaijanis for propaganda purposes.[38] The result was an invigorated war effort by Azerbaijan and a gravely deteriorating Armenian will to fight through the constant reliving of events and fear of unexpected future drone strikes.[39] The kinetic effects of drone strikes are lost lives and destroyed equipment, already damaging to the morale of a targeted belligerent. However, the ability of the drones to capture live full-motion video (FMV) and immediately broadcast this footage to online social media forums create powerful synergies between the kinetic and cognitive effects of unmanned aerial systems. Effects from these unmanned aerial systems cause both physical and psychological deterioration of their intended prey. Azerbaijan used FMV footage to amplify wisely what could be classified as the highly survivable kinetic effects of these weapons. Eventually, the Armenian war effort was crippled after a series of defeats displayed TB2 drones "literally flying circles near three S-300 sites while waiting to strike their targets before doing damage assessment and flying away," forcing the Armenian Army to capitulate rapidly.[40]

The Russian-backed Armenian Army was powerless to counter the effects of these Turkish and Israeli unmanned aerial systems (UAS). Ukraine, with which Russia has been in direct conflict since 2014, noticed this.[41] In September 2021, Ukraine acquired 24 TB2 drones from Turkey to bolster its own efforts against Russia after observing their effectiveness in the Second Nagorno-Karabakh War.[42] The following month, the Ukrainians deployed the TB2s against Russian-backed separatists in Crimea for the first time, damaging a 122mm D-30 howitzer in the Donbass region that had previously injured one Ukrainian soldier and killed another.[43] The Ukrainians followed the Azerbaijan example by using the onboard camera systems

to collect and distribute footage of the air strike online.[44] The Ukrainian Army employed this capability with continuously devastating effect after the Russian invasion in February 2022. While this is the most recent example of lessons from the Second Nagorno-Karabakh War's proliferation, it likely represents an early look at how future wars may be fought.[45] This deadly combination of conventional weaponry and narrative shaping tools represents a dangerous threat for states that fail to develop methods for controlling digital exhaust such as drone footage of engagements, especially battlefield losses.

## BULK DATA COLLECTION AND SALES

Bulk data collection refers to the mass collection of personal data gathered by social media companies and other website managers.[46] As users browse websites and services that require them to accept "informed consent" agreements coupled with the proliferation of Internet of things (IoT) devices when creating or linking personal accounts, the providers and creators of these services collect bulk data from their browsing patterns.[47] Two types of research typically employ these data: academic and marketing.[48] Marketing research practices in particular represent the greatest threat from bulk data collection, as this type of research usually involves the construction of personalized profiles of each individual user to monitor and record that person's likes, dislikes, interests, purchases, media preferences, and a variety of other traits.[49] While almost all web browsing generates bulk data, social media websites represent the prime collection ground for these data as they offer a look into not only a person's preferences, but also who they associate with, social movements with which they identify , and their personal beliefs.

This process, defined as "microtargeting" by MAJ Jessica Dawson,[50] represents a gold mine from a marketing perspective, as companies can use these data to construct carefully tailored advertisement intended to lure consumers into viewing and purchasing their products. However, from a security standpoint, microtargeting represents a potential narrative nightmare, as it offers anyone with access to this detailed profile information a roadmap for how best to propagandize messages in a way that will convince its target audience to adopt a desired perspective.[51] The Cambridge Analytica case demonstrates the potential for influencing operations based on the "digital exhaust" of users in the form of bulk data intentionally used to microtarget for the purpose of influencing "likely voter" decisions.[52] Both civilians and military personnel are vulnerable to microtargeting practices regardless of their social media use because, "even if an individual does not have a Facebook account, Facebook has a shadow account for them, collected from friends' phones, contacts lists, and emails as well as data Facebook itself purchases."[53] Usually, the only significant barrier to accessing these data is a licensing fee, meaning foreign adversaries can easily acquire them for nefarious purposes.

The same adversaries may also be able to amplify their microtargeted messages to a large audience of military personnel and civilians using "a relatively novel and increasingly dangerous means of persuasion within social media," which Lt Col Jarred Prier calls "commanding the trend."[54] This method involves using bot-driven, falsified swarms of activity or "views" to manipulate the algorithms that social media sites use to "analyze words, phrases, or hashtags to create a list of topics sorted in order of popularity."[55] This activity swarm increases a page's visibility and its likelihood of being clicked and shared by convincing social media algorithms that a topic is growing in popularity, prompting the algorithm to promote it on trending pages.[56] Algorithms do not verify the authenticity of stories before promoting them, nor do they verify the credibility of the users who share them. While some companies have begun modifying their algorithms and attempting to find countermeasures to bot swarms, the reality remains that by the time a topic has reached the trending page it has already spread beyond containment.[57] Narratives promoted in this manner that are harmful to Army interests could prove dangerous and impossible to control.

## POLICY SUGGESTIONS

As Joint Chiefs of Staff Chairman General Mark Milley has argued, strategic competitors' increasing capability to "fight the US through multiple layers of stand-off in all domains" means that a "doctrinal evolution" of the American way of war is necessary.[58] The lessons demonstrated in conflicts in Ukraine, Iraq, and Armenia suggest that narrative victory is growing in importance and a continual trend in the future.[59] The doctrinal adjustments necessary for the U.S. Army to fortify itself properly for this changing dynamic of warfare will likely be complex and take time to implement, but they will be essential to victory in future conflicts. The Army is probably the greatest modern conventional warfighting force, but it will need to bolster its ability to shape narratives surrounding conflicts in which it becomes involved to ensure that its conventional victories translate into strategic success.

The modern soldier must become conscious of his or her role as General Krulak's "strategic corporal," straddling the line between warfighter and diplomat.[60] In addition to combat capabilities, a soldier must be well-trained for decision making, problem solving, and positive cultural interaction.[61] Soldiers must be prepared for the eyes of the world on social media to scrutinize any and every action they take. The fate of Army morale and its reputation in the global court of public opinion hinges on the individual warfighter's ability to project a positive image of the Army to further the nation's strategic objectives. It is worth emphasizing that this does not represent a call for any lowering in priority of traditional combat skills and training; it is rather a call to elevate the importance of cultural and linguistic training as well as social media literacy.[62] Basing warfighter evaluations on both combat ability and social skills represents one way of honing these skills among Army personnel.

Signature management vulnerabilities present significant risks to operational security (OPSEC). Improving signals management strategies has been identified as a crucial step in advancing the U.S. Marine Corps' (USMC) contemporary warfighting capabilities for future conflicts.[63] The Army should afford signature management the same importance. Addressing these risks demands a prompt solution to the problems of physical infrastructure and the digital exhaust of personnel. The primary threat in the physical domain comes from China's 5G-infrastructure proliferation through its Belt and Road Initiative.[64] Using NATO as a "forum for collaboration" and expansion of US owned and operated 5G infrastructure is an optimal potential solution.[65] While this initiative will likely require significant investment in 5G-technology development and construction, the US could employ these technologies and their distribution as a diplomatic tool for strengthening relationships with existing allies or building new relationships with potential strategic partners. The Army and NATO operations in allied regions would also enjoy the benefits of US owned 5G systems: safe, trusted, and secure communications technology that would fully support the OPSEC of US joint and coalition forces.

Digital exhaust control may be more difficult to accomplish. The Army's ban on the use of personal communication devices on the battlefield is a constructive step, as it helps prevent the possibility of telecommunications interception, movement tracking using mobile device signals, and exposure to enemy disinformation that might demoralize or misinform soldiers.[66] Taking steps to mask deployment information such as supply purchases that may leave physical or digital paper trails should also be a priority. Purchasing supplies through a third-party or "middle-man," buying supplies in smaller quantities rather than in bulk and sending supplies to deployment zones with warfighters rather than shipping them directly there separately all represent potential solutions. To address online propaganda campaigns such as those seen in the second Nagorno-Karabakh War and Ukraine, the Army might consider using trend hijacking techniques such as bot swarming, as detailed by Prier, to bury adversaries' social media campaigns.[67] The Army needs to develop tactics, techniques, and procedures (TTPs) that mirror the informational effects demonstrated by the TB2 Bayraktar's successes in both the second Nagorno-Karabakh and Ukraine conflicts. TTPs that enhance the synergies between powerful kinetic and psychological effects stemming from these platforms. Furthermore, worth considering is the recruitment of existing social media influencers to help promote the Army's narratives, encouraging warfighters who demonstrate social media proficiency to become a new breed of battlefield correspondent, or the establishment of a U.S. Information Agency similar to the one created by President Eisenhower in 1953 to address US influence strategy during the Cold War. Israel's efforts to recruit young, tech-savvy, female social media operatives from existing Israeli Defense Force (IDF) units represents a notable success in this area.[68]

The Army's approach to bulk data sales and collection must respect the limitations put in place by the Fourth Amendment to the U.S. Constitution. For this reason, direct collection of data on American citizens for the purpose of microtargeted narrative construction is not a possibility. Rather, as MAJ Dawson[69] suggests, it may be useful for the Army to establish limits on data collection through cooperation with social media companies. The prevention of data collection from accounts owned by service members and their families represents a good starting point.[70] The encouragement of more stringent limits on obtaining these data from social media companies and the permitted uses of the data also represents a potential point of collaboration between the Army and social media corporations.

## CONCLUSION

As the U.S. Army prepares for future conflicts, it becomes increasingly critical to consider the demonstrations of narrative power from the past and those unfolding in the present day. Winning future conflicts will mean winning narrative conflicts. To do that, the Army needs to adopt appropriate doctrinal changes related to information operations, public affairs, and cyber space operations. Tactical actions will shape strategic success, which emphasizes the need to train and equip warfighters as ambassadors of the Army's intentions and good will. Words, tweets, TikToks, Instagram posts, drone recordings, and any other microtarget-enabling media deemed "view-worthy" are the weapons of narrative conflicts. The Army must learn to leverage these weapons and deny them to strategic adversaries. This means limiting digital exhaust, cooperating with social media companies to undermine adversaries' ability to target US warfighters and citizens, and establishing a comprehensive public relations arm of the Army to promote its narratives on the ideological battleground. As conflict evolves, so too must the warfighter. It is time to forge an Army of influencers.

## DISCLAIMER

The views and opinions expressed in this paper are those of the author alone and do not reflect the official policy or position of the U.S. Department of Defense (DoD), U.S. Cyber Command, or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.

## NOTES

1. Niall Ferguson, *The Square and the Tower: Networks and Power, from the Freemasons to Facebook*, Penguin Books (2019).
2. Ibid.
3. Ibid.
4. David Patrikarakos, *War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century*, Hachette UK, (2017).
5. Ibid.
6. Sun Tzu, *The Art of War,* translated by Sammeul Griffith, Duncan Baird (2005, original work published 5th century BC), 108.
7. Peter warren Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Eamon Dolan Books (2018).
8. Ibid.
9. General Charles C. Krulak, T*he Strategic Corporal: Leadership in the Three Block War*, Center for Army Lessons Learned Fort Leavenworth KS Virtual Research Library (1999), 5.
10. Stephen Bochner, "The Social Psychology of Cross-Cultural Relations," in *Culture in Contact: Studies in Cross-Cultural Interaction*, edited by Stephen Bochner, Volume 1, Oxford: Pergamon (1982), 14.
11. Bochner, "The Social Psychology of Cross-Cultural Relations," 13; Krulak, *The Strategic Corporal.*
12. Bochner, "The Social Psychology of Cross-Cultural Relations," 15.
13. Kevin D. Stringer, "Educating the Strategic Corporal: A Paradigm Shift," *Joint, Interagency, Intergovernmental, and Multinational Newsletter* (2011), 65; Major Linda Liddy, "The Strategic Corporal: Some Requirements in Training and Education," *Australian Army Journal* 2, no. 2 (2004), 139-148.
14. Liddy, "The Strategic Corporal: Some Requirements in Training and Education," 142.
15. Patrikarakos, *War in 140 Characters.*
16. Charlie Winter, *Media Jihad: Islamic State's Doctrine for Information Warfare*, London, UK, International Centre for the Study of Radicalisation and Political Violence (2017).
17. Patrikarakos, *War in 140 Characters.*
18. Bochner, "The Social Psychology of Cross-Cultural Relations," 13; LTC Robert J. Ross, Creating White Space: Interaction and the Adaptation of Team Social Identity in Complex Environments, Naval Postgraduate School Monterey, Monterey CA (2019), 19.
19. Krulak, The Strategic Corporal.
20. Brett van Niekerk and M. S. Maharaj, "Mobile Devices and the Military: Useful Tool or Significant Threat?," *Journal of Information Warfare* 11, no. 2 (2012), 1-11.
21. Josh Rutland "A Military of Influencers: The U.S. Army, Social Media, and Winning Narrative Conflicts" [unpublished master's thesis], Augusta University.
22. Brian David Johnson, Alida Draudt, Jason C. Brown, LTC Robert J. Ross, Ph. D., "Information Warfare and the Future of Conflict," produced by Cyndi Coon, The 2019 Threatcasting Workshop, Arizona State University (2019), 68.
23. U.S. Army, *U.S. Army Techniques Publication 3-13.3: Army Operations Security for Division and Below*, Headquarters, Department of the Army (2019), 1-1.
24. Luiz A. Dasilva, Jeffrey H. Reed, Sachin Shetty, Jerry Park, Duminda Wijeskera, and Haining Wang, "Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation," *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (2020), 74-87.
25. Carolyn Bartholomew, "China and 5G," *Issues in Science and Technology* 36, no. 3 (2020), 50-57.
26. Ibid.
27. Ibid., 52-52.
28. Dasilva et al., "Securing 5G".
29. Ibid., 85.
30. Johnson et al., "Information Warfare and the Future of Conflict"; Rutland, "A Military of Influencers."
31. Matt Sienkewicz, "Open BUK: Digital labor, media investigation and the downing of MH17," *Critical Studies in Media Communication* 32, no. 3 (2015), 208-223; Patrikarakos, *War in 140 Characters.*

## NOTES

32. Patrikarakos, War in 140 Characters, 181.
33. Ibid.
34. Ibid. Eliot Higgins, We Are Bellingcat: Global Crime, Online Sleuths, And The Bold Future Of News, Bloomsbury Publishing (2021).
35. Higgins, We Are Bellingcat: Global Crime, Online Sleuths, And The Bold Future Of News.
36. John Antal, "The First War Won Primarily with Unmanned Systems: Ten Lessons from the Second Nagorno-Karabakh War" (2021), https://www.socom.mil/.
37. Ibid.
38. Ibid.
39. Ibid.; Stijin Mitzer and Joost Oliemans, "Aftermath: Lessons of The Nagorno-Karabakh War Are Paraded Through the Streets of Baku," Oryx (2021), https://www.oryxspioenkop.com/; Rutland, "A Military of Influencers."
40. Mitzer and Oliemans, "Aftermath: Lessons of The Nagorno-Karabakh War Are Paraded Through the Streets of Baku," para. 22.
41. Burak Ege Bekdil, "Ukraine is set to buy 24 Turkish drones. So why hasn't Russia pushed back?" *Defense News* (September 29, 2021), https://www.defensenews.com/unmanned/2021/09/29/ukraine-is-set-to-buy-24-turkish-drones-so-why-hasnt-russia-pushed-back/.
42. Ibid.
43. Joseph Trevithick, "Ukraine Strikes Russian-Backed Forces Using Turkish-Made TB2 Drones For The First Time," *The Drive* (October 27, 2021), https://www.thedrive.com/the-war-zone/42894/ukraine-strikes-russian-backed-forces-using-turkish-made-tb2-drones-for-the-first-time.
44. Antal, "The First War Won Primarily with Unmanned Systems;" Trevithick, "Ukraine Strikes Russian-Backed Forces Using Turkish-Made TB2 Drones For The First Time."
45. Stephen Witt, "The Turkish Drone That Changed The Nature Of Warfare," *The New Yorker* (May 9, 2022), https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare.
46. Rutland, "A Military of Influencers."
47. Trang Tran, "Personalized ads on Facebook: An effective marketing tool for online marketers," *Journal of Retailing and Consumer Services* 39 (2017), 230-242.
48. Ralph Schroeder, "Big Data and the brave new world of social media research," *Big Data & Society* 1, no. 2 (2014), 2.
49. Tran, "Personalized ads on Facebook."
50. Major Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* 6, no. 1 (2021), 63-80.
51. Ibid.
52. Jim Isaak and Mina J. Hanna, "User data privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* 51, no. 8 (2018), 56-59; Dawson, "Microtargeting as Information Warfare."
53. Dawson, "Microtargeting as Information Warfare," 72.
54. Lt Col Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017), 51.
55. Ibid., 52.
56. Ibid.
57. Rutland "A Military of Influencers."
58. "The U.S. Army in multi-domain operations 2028," Fort Monroe, VA: Army Training and Doctrine Command (2018), 3.
59. Irina Khaldrova and Mervi Pantti, "Fake News: The Narrative Battle Over the Ukrainian Conflict," *Journalism Practice* 10, no. 7 (2016), 891-901; Singer and Brooking, *LikeWar;* Antal, "The First War Won Primarily with Unmanned Systems".
60. Krulak, *The Strategic Corporal.*
61. Ibid.
62. Stringer, "Educating the Strategic Corporal".
63. Capt. Luke Klena, "Technical Signature management for Small Units," *Marine Corps Gazette,* May 2021 (2021).

## NOTES

64. Dasilva et al., "Securing 5G."
65. Ibid., 85.
66. Singer and Brooking, *LikeWar;* Van Niekirk and Maharaj, "Mobile Devices and the Military."
67. Prier, "Commanding the Trend."
68. Patrikarakos, *War in 140 Characters.*
69. Dawson, "Microtargeting as Information Warfare."
70. Ibid.