The Information Domain and Social Media

SGM ALEXANDER E. AGUILASTRATT
SGM MATTHEW S. UPDIKE

A form of asymmetric warfare is waged against the United States and its citizens daily across multiple venues and platforms without reaching the threshold or definition of open conflict.[1] That form of asymmetric warfare is disinformation.

Disinformation erodes trust and the ability to establish a society with effective institutions to serve and protect. As a result, it is conceivable to assume that disinformation and its social-media venues are corrosives affecting the information domain.

Much like the early stages of improvised explosive devices (IEDs), disinformation presents the United States with a cost-effective, low-effort tactical problem with a strategic consequence manifested in national trust erosion. The U.S. Army faces the renewal of great power competition with adversaries engaging in multiple domains, thus challenging the traditional definitions of war and peace and operating under the threshold that would warrant military action.[2]

Graphic by Patrick Buffett

Social media is the preferred venue for foreign, domestic, and proxy enemies to engage the Army remotely with minor risk.

A few years ago, Frank Hoffman identified the "weaponization" of social media as playing perfectly into the concept of hybrid warfare: "[Hybrid warfare] incorporates a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."[3]

Importance

The information domain offers adversaries the ability to engage the U.S. Army with digital IEDs and erode trust between our military and the American people. Social media is the preferred venue for foreign, domestic, and proxy enemies to engage the Army remotely with minor risk.

The information domain starts at the tactical level, and it is also a tactical commander's responsibility to occupy it or otherwise relinquish key terrain to nefarious actors. However, there is a lack of concise guidance about information and the aspects of cross-domain warfare. The result is the effect of "paralysis by analysis" and the consequent disregard of social media as a tactical system in the new information domain.

Active measures in the realm of social media include influencing others in a coercive way; disinformation; political-influence operations in what could be considered the tactical setting for the asymmetric gray zone; hybrid; or next-generation information warfare against the U.S. Army.

Operational Environment

Social media, as part of the information domain, fits perfectly as a tool to shape the information operational environment, coordinate efforts, and erode trust by antagonizing below the threshold of conflict.[4]

In the past, basic communication models included sender, receiver, transmission, medium, and message as separate components; however, due to advances in technology, the information domain now adds the Internet, radio waves, satellite communications, wireless networks, and social media to the previous media.[5]

As a result, the information domain will become the preferred operational environment by near-peer, extremist organizations, and domestic threats that cannot match the U.S. Army's kinetic capabilities.

Example: ISIS in Mosul

When the Islamic State of Iraq and Syria (ISIS) invaded Northern Iraq in 2014, it only had about 15,000 militants who picked up weapons and vehicles from the previous extremist groups. However, after introducing its hashtag campaign #ALLEyesOnISIS, it gained an extensive network of passionate supporters and Twitter bots to lock down other trending hashtags for Arabic-speaking users.[6] ISIS' on-line tactics and mastery of the information domain recruited from more than 100 countries and spread fear globally.

The information domain as an operational environment is now a contested battlespace where various actors with real-world goals such as ISIS could use the same tactics with relative simplicity. For example, ISIS's top recruiter, Junaid Hussein, used the same tactics that Taylor Swift used to sell her records.[7]

The acknowledgment of the changes in the character of warfare related to the information domain is evident not only to the military but also to corporations. Facebook, for example, is planning the creation of a "war room" to counter disinformation operations.[8]

Commanders at all levels deal with the challenges of the information domain, social media, and their formations. Social media is the ideal platform for information/disinformation, on-line communities, nefarious actors, inundation and targeting, and less-than-honest techniques. For example, during the last Mexican elections, one-third of the on-line conversations were generated by bots.[9]

Social-media platforms are addictive by design. Notifications, for example, do not tell the user what the subject is about, thus creating a certain level of anxiety and the need for closure, appealing to emotions. Unfortunately, our young generation of Soldiers is affected by this type of emotional targeting. For example, in Chicago, 80 percent of school fights originate from on-line comments. Gangs and extremist-organization recruiters stir negative emotions such as anger to disenfranchise and absorb young recruits.

If units do not occupy and employ the information-domain operational environment, they risk enabling nefarious actors to target Soldiers, spread disinformation, and operate with impunity.

Speed and Level of Response

The need for a social-media presence as part of information-domain occupation is paramount for U.S. society and its symbiotic relationship of trust with its Army. One of the most efficient ways for commanders to occupy the information domain and counter disinformation is to practice consistent messaging, whether doctrine or science/fact-based.

As social media continues to evolve with visual venues, including China's TikTok, it is essential to point out that the enemy uses artificial intelligence and algorithms to flood the virtual battlefield. As a result, reliable information must be treated as a defensive/offensive weapon system and an area-denial tool against threat actors.

> ***The U.S. Army must recognize at echelon that social media can be used as a weapon of adverse effects; therefore, it must invest in social-media literacy and instill awareness of methods and goals of targeted campaigns by nefarious actors.***

The most effective tool against nefarious actors is an educated and empowered population of Soldiers and leaders capable of identifying and discrediting disinformation attempts. The U.S. Army must recognize at echelon that social media can be used as a weapon of adverse effects; therefore, it must invest in social-media literacy and instill awareness of methods and goals of targeted campaigns by nefarious actors.

For example, Russia believes that the United States' weakness is its diversity, so to counter this, the U.S. Army must show strength in its pluralism and pave the way to heal the divisions in our country by shielding our own culture. When the Army acknowledges social media as part of the information domain and develops an effective strategy, it will deny nefarious actors crucial terrain in the information environment.

Changes in Technology

The U.S. Army's adversaries see information as a domain and all forms across platforms as potential venues of power ready to be weaponized. Near-peer threats also view all U.S. information-technology systems as vulnerabilities.[10]

As information technology evolves, so do its platforms (using TikTok as an example). Technological advances enable nefarious actors to manipulate media with artificial intelligence-enabled "deep fakes."[11] Tech companies are developing methods to reveal such deep fakes and image alterations that create anger and negative public opinion.

Also, developers are working on their algorithms to counter those used by nefarious actors to discourage the practice of sharing misleading information based on the title alone. The algorithms will aid in creating a healthy level of skepticism, improving social-media literacy.[12]

Despite all advances in technology, the most important advance must occur within the human domain. The most effective tool to counter disinformation and divisionism is the educated and empowered U.S. Army, capable of discrediting disinformation and targeting efforts. In addition, the Army must inoculate its Soldiers against those who seek malign control of the information domain.

Command teams must invest in social-media literacy and instill awareness, methods, and goals of targeted disinformation campaigns while measuring fissures in their information campaigns.

Strategic Communications and Information Advantage

The spread of misinformation and division is actually a "biohazard" that can spread throughout any formation if command teams do not effectively occupy the information domain. Command teams at echelon must define purpose with clarity and convey clear and concise messaging while considering the target audience and desired effects to counter or deny the enemy of crucial terrain to infect the information domain.

Social media is an effective platform to inform Soldiers and families while combating disinformation. Also, young Soldiers, officers, and NCOs live in an era in which social media is essential in their lives.

Humanizing the narrative to create positive effects within formations is critical for countering the infection created by the weaponization of social media. Units that humanize their narrative can use the information domain as a means for Soldiers to:

- Know the unit's purpose;
- Communicate that purpose often and in different ways;
- Make it personal by creating informal feedback loops;
- Reinforce narrative with actions;
- Give purposed-based feedback; and
- Align behaviors with purpose.

Pre, During, and After Action Plans

Effective social-media communication provides command teams a venue to exercise information-domain advantage and deny nefarious actors key terrain and avenues to infect formations. Also, command teams and staff must have the capability to engage in contingency operations to inform or respond to emergencies before, during, and after crises.

Time is of the essence, especially if that time is during a crisis. You will likely use social media and on-line platforms as the first resource to react and to put out information. Because social media provides speed, reach, and direct contact with audiences, it is a crucial tool to disseminate command information and provide a place to receive timely updates.

Develop the social-media strategy as part of your crisis-communication plan. Having a set strategy the team is comfortable with will help your unit better prepare and manage responses during a crisis.

Command Presence and Talent Management

Command teams must manage the information domain like any operational environment. Staff and senior enlisted advisers can help the commander navigate the complex environment using experienced members within their formation (Soldiers and civilians) who are talented and adept to the social-media environment. A candid, genuine command presence can help leaders define their expectations, style, and expectations to Soldiers and geographically displaced family members.

Also, subordinate commanders can emulate a solid and genuine social-media command presence. Defining leader expectations for the information domain is as important and comparable to the four rules of a gun range:

- Watch the muzzle and keep it pointed in a safe direction at all times;
- Treat every weapon system as if loaded at all times;

Vignette: Social-Media Reputation Management and Response (10th Mountain Division Shoothouse Incident, 21 February 2021)

A bodycam video of Soldiers conducting live-fire close-quarters battle training displaying many safety violations began circulating on the Internet. It claimed that the Soldiers belonged to 10th Mountain Division.

Staff from the 10th Mountain determined the Soldiers were from the division but not the unit they belonged to or how long ago the training occurred.

Measured response: Within 24 hours, the video had gone viral. Through contact with the meme pages from the energy-drink rumor, CSM Mario O. Terenas, 10th Mountain's top enlisted Soldier, eventually determined the exact unit in the shoothouse and the training time. Rather than send out an old-fashioned press release, he addressed the allegations in a one-minute response video on all his social-media accounts.

He admitted that the Soldiers belonged to 10th Mountain Division and was saddened by what he saw. However, he assured the audience that was not the unit's standard and he would fix the problem.

Results: CSM Terenas' video received an overwhelming amount of audience engagement. Users commended Terenas for owning up to the allegations instead of trying to hide from them. His video went viral almost immediately after being released (152,000 views on Twitter, 86,000 Instagram views, and 1,000 on Facebook).

- Positively identify the target and the backdrop; and
- Keep your finger off the trigger until ready to engage.

Social media is an excellent medium for sharing information and reaching out to otherwise geographically displaced personnel; however, it is also a target-rich environment for nefarious actors. As a result, a strong command presence, coupled with action plans and expectations, is required to protect command integrity and safeguard Soldiers and families from the effects of disinformation and deliberate targeting.

Threats

Foreign. Open-source intelligence indicates that foreign actors are engaging in covert information operations against the United States. Disinformation is not a new concept. Russia has a long history of seeking to project power and influence while playing to our potential technological and geopolitical handicaps.[13]

Without the equivalent conventional might of the United States, Russia, China and other nations recognize our appetite for information. They use social media as a platform to exercise tactics of influence, coercion, and the capability to control the narrative, thus manipulating a specific population's hearts and minds.[14]

The diverse, pluralistic, and democratic nature of the United States makes it a target-rich environment of social-media-empowered Russian disinformation. As a result, the all-volunteer force composed of free citizens of a diverse nation offers the same opportunities for a country that has long fought to rebalance power.[15]

At the macro level, Russia has realized U.S. conventional superiority, with General Valery Gerasimov's doctrine revolving around information control as the key to victory. The Gerasimov Doctrine — or Russian new-generation warfare — advocates simultaneous operation and control of the military, political, cyber, and information domains, which can be accessed employing social media.[16]

Gerasimov also made the following statement about information technology: "Information technology is one of the most promising types of weapons to be used covertly not only against critically important informational infrastructures but also against the population of a country, directly influencing the condition of a state's national security."[17]

Russia operates under the concept that the distinction between war and peace no longer exists and uses misinformation to protect itself from a military response. In essence, once it has started, Russia must maintain momentum since it acknowledges that the United States' advantages in information technology will undermine Russian social, cultural, and political institutions if pushed beyond the threshold of conflict.[18]

China also seeks to influence the American public, although its approach differs widely from Russia's tactics. A Recorded Future article stated: "We believe that the Chinese state has employed a plethora of state-run media to exploit the openness of American democratic society in an effort to insert an intentionally distorted and biased narrative portraying a utopian view of the Chinese government and party. ...what distinguishes Russian and Chinese approaches are their tactics, strategic goals, and efficacy."[19]

A paper published by the Hoover Institution in November 2018 included findings from more than 30 of the West's preeminent China scholars, collaborating in a working group on China's influence operations abroad. The scholars concluded: "[T]his report details a range of more assertive and opaque 'sharp power' activities that China has stepped up within the United States in an increasingly active manner. These exploit the openness of our democratic society to challenge, and sometimes even undermine, core American freedoms, norms, and laws."[20]

> *"The Russian state has used a broadly negative, combative, destabilizing, and discordant influence operation because that type of campaign supports Russia's strategic goals to undermine faith in democratic processes, support pro-Russian policies or preferred outcomes, and sow division within Western societies. Russia's strategic*

goals require covert actions and are inherently disruptive, therefore, the social-media influence techniques employed are secretive and disruptive as well.

The Chinese state has a starkly different set of strategic goals, and as a result, Chinese state-run social-media influence operations use different techniques. [Chinese President] Xi Jinping has chosen to support China's goal to exert greater influence on the current international system by portraying the government in a positive light, arguing that China's rise will be beneficial, cooperative, and constructive for the global community. This goal requires a coordinated global message and technique, which presents a strong, confident, and optimistic China."[21]

Graphic by Regina Ali

Military experts are constantly warning service members about social media scams.

The relentless need to maintain the social media and disinformation continuum of operations under the destabilizing Gerasimov Doctrine enables Russian tactical commanders to conduct offensive cyber and information operations. In contrast, U.S. tactical commanders lack clear social-media guidance at the tactical level. It is fair to conclude that a Russian tactical commander is more empowered to conduct offensive information operations than a U.S. tactical-level commander due to the protection of several disinformation layers. As a result, Russian tactical-information units and their proxies occupy the proverbial "high ground" of the information domain.

Modus operandi. Western newspapers once described Russian President Vladimir Putin as "the cold-eyed ruler of Russia," "a cold, calculating … spy who sought to undermine freedom in the West." With "his dark past, his sinister look," he was "straight out of KGB central casting."[22] Thus one could say that Putin is the spy who would be king. As such, he understood that once he embarked on the Gerasimov Doctrine, his methods for occupying the information domain would become predictable.

As a result, the need for relentless action at the tactical level would become the Russian apparatus' cornerstone. Therefore Russia's social-media exploitation method is predictable. They identify a contentious issue, employ bots and trolls on various social-media platforms to spread divisive messages, and amplify discord.[23]

In addition, a diverse U.S. Army, recruiting from a pluralistic society dealing with societal fissures and racial tension, creates opportunities for Russian disinformation attacks against the foundations of trust between the U.S. Army and the American people.

In the case of creating friction against the U.S. Army, Russia employs tactics such as those used against African-Americans in advance of the 2016 election and the exploitation of the Black Lives Matter movement by flooding Twitter hashtags and diluting legitimate concerns.[24]

The need for a response and occupation of the information domain becomes prevalent when the Russian threat recognizes the need to identify, exploit, and amplify U.S. political tensions, racial wounds, and the promotion of health scams (anti-vaxxer movement) in a divisive and emotional manner.

Domestic. On-line social-media platforms are playing an increasingly important role in the radicalization processes of U.S. extremists. While U.S. extremists were slow to embrace social media, in recent years the number of individuals relying on these user-to-user platforms to disseminate extremist content and the facilitation of extremist relationships has grown exponentially.

In fact, in 2016 alone, social media played a role in the radicalization processes of nearly 90 percent of the extremists in Profiles of Individual Radicalization in the United States data.

Social media exists for the extremist the same way it exists for the everyday user, neither evil nor benevolent. Social-media sites are simply a method extremists use to conduct a myriad of organizational functions.

Facebook, Twitter, or YouTube are the most popular social-media sites today, but that does not mean they will stay on top. Tumblr, LinkedIn, Google+, and Instagram are all social-media sites growing in popularity.

Command teams and staff must acknowledge and keep abreast of new advances in social media.[25] However, it must not consume their time, nor should they neglect professional distance, but rather consider social media as part of the information domain.

Notes

[1] Sarah Jacobs Gamberini, "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns," *Joint Force Quarterly*, 4th Quarter 2020.

[2] Ibid.

[3] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies, 2007), cited in Dr. Ofer Fridman, "The Danger of 'Russian Hybrid Warfare,'" Cicero Foundation Great Debate Paper, July 2017.

[4] Gamberini, "Social Media Weaponization."

[5] Robert Kozloski, "The Information Domain as an Element of National Power," Center for Contemporary Conflict, 2020.

[6] The University of Pennsylvania, "Why Social Media is the New Weapon in Modern Warfare," Knowledge@Wharton interview with P.W. Singer and Emerson T. Brooking, 2019.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Gamberini, "Social Media Weaponization."

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Dr. Harold Orenstein and LTC (Retired) Timothy Thomas, "The Development of Military Strategy Under Contemporary Conditions: Tasks for Military Science," *Military Review*, November 2019.

[18] Gamberini, "Social Media Weaponization."

[19] Recorded Future, "Beyond Hybrid War: How China Exploits Social Media to Sway American Opinion," 6 March 2019, accessed from https://www.recordedfuture.com/china-social-media-operations.

[20] Larry Diamond and Orville Schell, eds., "China's Influence & American Interests: Promoting Constructive Vigilance," The Hoover Institution, 29 November 2018, accessed from https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance.

[21] Recorded Future, "Beyond Hybrid War."

[22] Greg McLaughlin, *Russia and the Media: The Makings of a New Cold War* (London: Pluto Press, 2020); retrieved from http://www.jstor.org/stable/j.ctvzsmdt1.

[23] Gamberini, "Social Media Weaponization."

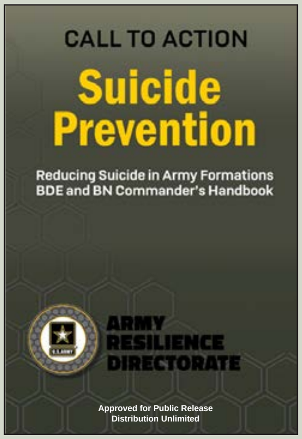
[24] Ibid.

[25] U.S. Air Force MAJ Joshua Close, "#Terror: Social Media and Extremism," paper for graduate requirements, Air Command and Staff College, May 2014.

Editor's Note: *This article first appeared in the Winter 2022 issue of* Armor.

SGM Alexander Aguilastratt is an Infantry Soldier assigned as the U.S. Army Training and Doctrine Command (TRADOC) project-inclusion sergeant major at the Pentagon, Washington, D.C. His previous assignments include serving as command sergeant major, U.S. Southern Command, Soto Cano Air Force Base, Honduras; command sergeant major, Charlie Squadron, Asymmetric Warfare Group (AWG), Fort Meade, MD; and sergeant major, Baker Squadron, AWG, Fort Meade. His military schooling includes the U.S. Army Sergeant Major Academy, Vulnerability Assessment Methodology Course, AWG Operational Adviser Training Course, Master Resiliency Course, Joint Readiness Training Center Observer-Controller Course, Reserve Officer Training Command Course, Air Assault School, Airborne School, and Jumpmaster Course. SGM Aguilastratt earned a master's degree in international relations and affairs from Liberty University and a bachelor's degree in business administration in liberal arts (graduated summa cum laude) from Excelsior College.

SGM Matthew Updike has a scout background. At the time this article was written, he was assigned to G-3/5/7, TRADOC, Fort Eustis, VA. His previous assignments include serving as command sergeant major for deputy director, Noncommissioned Officer's Professional Development Directorate, NCO Center of Excellence, Fort Bliss, TX; brigade command sergeant major, Task Force Sinai, Sharm el-Sheikh, Egypt; and command sergeant major, 3rd Squadron, 71st Cavalry Regiment, 1st Brigade Combat Team, 10th Mountain Division, Fort Drum, NY. His military schooling includes the Scout Leader Course, security force assistance advisor training, Sergeants Major Course, and Maneuver Battalion and Brigade Pre-Command Course. SGM Updike earned an associate's degree in business and administration and a bachelor's degree in business and management from Excelsior College.



CALL TO ACTION
Suicide Prevention
Reducing Suicide in Army Formations
BDE and BN Commander's Handbook
ARMY RESILIENCE DIRECTORATE
Approved for Public Release
Distribution Unlimited