



SOCIAL MEDIA

IS CHANGING THE WAY THE **ARMY** COMMUNICATES.



WWW.FACEBOOK.COM/USARMY
WWW.TWITTER.COM/USARMY
WWW.INSTAGRAM.COM/USARMY
WWW.YOUTUBE.COM/USARMY

LIKE US. FOLLOW US. WATCH US... **CONNECT!**

(U.S. Army graphic)

The Information Domain and Social Media: Part 2

By Sgts. Maj. Alexander Aguilastratt, Matthew Updike, & Montigo White

U.S. Army Training and Doctrine Command

In continuing the conversation about social media and its relevancy in modern times for multiple generations, it must be stated that first and foremost, it is an excellent medium for sharing information between friends, family, and coworkers. However, it is also a target-rich environment full of unprepared or unwitting organizations and users. This article, second in a two-part series, describes communication plans, the importance of command presence, current threats, and what to look out for to keep organizations and users safe.

Strategic Communications and Information Advantage

Social media platforms are an effective space to combat disinformation and keep Soldiers and families informed. Command teams at echelon must define their purpose with clarity and convey clear and concise

messaging while considering their target audience and desired effects to counter or deny an enemy's disinformation throughout the domain. Additionally, young Soldiers, officers, and NCOs live in an era where social media is an integral part of their lives, so it's important to embrace the positive and prepare for its negative effects because it's not going away.

Creating positive effects within formations is critical for countering social media weaponization by our adversaries. Some easy steps to prepare your unit for positive social media usage are:

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

Pre, During and After-Action Plans

Effective command team social media communication 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 during an important or catastrophic event. The command team will likely use social media and online platforms first to put out information because it is fast, has a wide reach, and provides direct contact with audiences. It is a crucial tool to disseminate command information and provide a place to receive timely updates. It is important to develop a social media strategy early as part of your crisis communication plan. Having the team comfortable with a set strategy will help your unit better prepare to use and manage responses during a crisis.

Real World Example:

10th Mountain Division Shoot House Incident, Feb. 21, 2021.

A body camera video of Soldiers conducting live-fire close quarters battle training displaying numerous safety violations began circulating on the internet. It claimed the Soldiers belonged to the 10th Mountain Division. However, 10th Mountain staff 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. 10th Mountain Division's command sergeant major eventually determined the exact unit in the shoot house 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 the Soldiers belonged to the 10th Mountain Division and was saddened by what he saw. However, he assured the audience that was not the unit's standard and the problem would be fixed.

Results: The video received overwhelming audience engagement. Users commended the command sergeant major for owning up to the allegations instead of trying to hide from them. His response went viral almost immediately after being released. (152K views on Twitter, 86K Instagram views, and 1K on Facebook)

Command Presence and Talent Management

Command teams must treat the information domain like any other operational environment. Staff and senior enlisted advisers can help the commander navigate the domain using experienced members within the formation—Soldiers and civilians. A candid, genuine command presence can help leaders define their expectations and style to Soldiers as well as geographically displaced family members.

Threats

Foreign

Open-source intelligence indicates that foreign actors engage in covert information operations against the U.S. Russia has a long history of projecting power and influence while playing to our potential technological and geopolitical handicaps (Gamberini, 2020). Without the equivalent conventional might of the U.S., Russia (though still an existential threat) recognizes our appetite for information. It uses social media to influence, coerce, and control the narrative, thus manipulating a specific population's hearts and minds (Kelly & Samuels, 2019). The diverse, pluralistic, and democratic nature of the U.S. makes it a target-rich environment for Russia's social media-empowered disinformation campaigns.

At the macro level, Russia realized the U.S. has conventional superiority but General Gerasimov's doctrine focuses on information control as the key to victory. The Gerasimov Doctrine, or Russia New Generation Warfare, advocates for simultaneous operation and control of the military, political, cyber, and information domains (Gamberini, 2020), which can be accessed employing social media. In Gerasimov's doctrine:

“Having no clearly expressed national borders, the information sphere provides the possibility of remote, covert effects 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. It is namely for this reason that the study of issues of preparing and conducting information operations is a very important task for military science” (Orenstein & Thomas, 2019, para. 52).

Russia's relentless need to maintain the social media and disinformation operations under the Gerasimov Doctrine enables their tactical commanders to conduct offensive cyber and information operations. In contrast, U.S. tactical commanders often lack clear social media guidance at the tactical level. As a result, Russian tactical information units, and their proxies, currently occupy the proverbial “high ground” in the information domain.

Modus Operandi

Western newspapers describe Russian President Vladimir Putin as the cold-eyed ruler of Russia, “a cold, calculating...spy who sought to undermine freedom in the West...his dark past, his sinister look...straight out of KGB central casting” (McLaughlin, 2020, p. 33). Putin understands that once embarked on the Gerasimov Doctrine, his methods for occupying the information domain become predictable. As a result, the need for relentless

action at the tactical level became the Russian apparatus's cornerstone, making their social media exploitation methods predictable. They identify a contentious issue, employ bots and trolls on various social media platforms to spread divisive messages, and amplify discord (Gamberini, 2020). For example, in order to cause friction within 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 (Gamberini, 2020).

The need to respond and employ the information domain becomes a priority when our enemies recognize our vulnerabilities and can identify, exploit, and amplify U.S. political tensions, racial wounds, and divisive issues such as the anti-vaxxer movement.

Domestic

Online social media platforms play an increasingly important role in the U.S. extremist radicalization processes. While extremists were slow to embrace social media, in recent years, the number of individuals relying on these user-to-user platforms to disseminate their radical content and facilitate extremist relationships has grown exponentially. In fact, in 2016 alone, social media played a role in the radicalization processes of nearly 90% of the extremists in the U.S. ("National Consortium," 2018).

Social media exists for extremists the same way as for everyday users, neither good nor evil. Social media websites are simply a method extremists use to conduct a myriad of organizational functions. Facebook, Twitter, and YouTube are the most popular sites today, but that does not mean they will remain so. TikTok, Tumblr, Linked In, and Instagram are all social media sites growing in popularity. Command teams and staff must acknowledge and keep abreast of new social media advances and platforms to stay relevant and prepared (Close, 2014).



THINK ABOUT WHAT MESSAGE IS BEING COMMUNICATED AND WHO COULD POTENTIALLY VIEW IT.

TYPE MESSAGES THAT ARE CONSISTENT WITH OUR U.S. ARMY VALUES.

POST IF THE MESSAGE DEMONSTRATES DIGNITY AND RESPECT FOR SELF AND OTHERS.

"When engaging in social media, Army team members should apply the 'think, type, post' methodology," wrote Robert Speer while serving as acting Secretary of the Army in 2017. (U.S. Army graphic)

Conclusion

Command teams must be knowledgeable about social media practices and must be aware of the methods and goals of targeted disinformation campaigns while measuring the effectiveness of their information campaigns. Evolving and educating the human domain is an essential weapon against those who wish the U.S. harm. Ultimately, we must remember 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. ■

References

- Close, J. (2014). #Terror Social Media and Extremism. *Air Command and Staff College*.
- Gamberini, S. J. (2020). Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns. *Joint Force Quarterly*, 5(99).
- Kelly, M. & Samuels, E. (2019). How Russia weaponized social media, got caught and escaped consequences. *The Washington Post*. <https://www.washingtonpost.com/politics/2019/11/18/how-russia-weaponized-social-media-got-caught-escaped-consequences/>
- McLaughlin, G. (2020). Putin is Russia. In *Russia and the Media: The Makings of a New Cold War* (p. 33). London: Pluto Press. <http://www.jstor.org/stable/j.ctvzsmtdt1>
- National Consortium for the Study of Terrorism and Responses to Terrorism. (2018). (rep.). *The Use of Social Media by United States Extremists*. Retrieved January 21, 2022, from <https://safe.menlosecurity.com/doc/docview/viewer/doc-N95E37103E96B4dd850a13a803a01eb115238c32a9dfe-694ce61a95bce70b7d372857ba480006>
- Orenstein, H., & Thomas, T. (2019). The Development of Military Strategy Under Contemporary Conditions: Tasks for Military Science. *Military Review*. <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2019-OLE/November/Orenstein-Gerasimov/>

Sgt. Maj. Alexander Aguilastratt is the U.S. Army Training and Doctrine Command (TRADOC) liaison to Headquarters, Department of the Army, and the TRADOC Project Inclusion sergeant major. Aguilastratt previously served as the Charlie Squadron, Asymmetric Warfare Group's command sergeant major as well as Joint Task Force-Bravo command sergeant major.

Sgt. Maj. (Ret.) Matthew Updike most recently served with the Enlisted Initiatives Group, TRADOC. His previous assignments include Director NCO Professional Directorate at the NCO Leadership Center of Excellence and Task Force Sinai, Egypt. He is a graduate of the U.S. Army Sergeants Major Academy (Class 66).

Sgt. Maj. Montigo White is the senior enlisted advisor for the TRADOC Communication Directorate. He has served in a multitude of public affairs positions to include photographer for the Office of the Secretary of the Army, 24th Press Camp Headquarters command sergeant major., and the Defense Information School command sergeant major.



<https://www.armyupress.army.mil/Journals/NCO-Journal/>

<https://www.facebook.com/NCOJournal>

<https://twitter.com/NCOJournal>

Disclaimer: The views expressed in this article are those of the authors and do not necessarily reflect the opinions of the NCO Journal, the U.S. Army, or the Department of Defense.

