It is important for military personnel to remember that when they're logged on to a social media platform, they still represent their respective branch of service and must abide by the Uniform Code of Military Justice at all times, even when off-duty. (U.S. Army graphic by Patrick Buffett)

The Information Domain and Social Media: Part 1

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

U.S. Army Training and Doctrine Command

"If the first wars were fought with sticks and stones, modern warfare is a high-tech battlefield where social media has emerged as a surprising — and effective — weapon. From Russian hacking to influence the American election to online recruitment for terror groups such as ISIS, an array of players are using false news and bogus accounts to stoke fear, incite violence and manipulate outcomes." ("Why social media is the new weapon," 2019, para. 1)

A form of asymmetric warfare is waged against the U.S. daily across multiple platforms without reaching the threshold or definition of open conflict (Gamberini, 2020). As a result, we should assume that disinformation across social media services are corrosively affecting the information domain. Much like the early stages of the Improvised Explosive Device (IED) in Iraq and Afghanistan, it presents the U.S. with a tactical problem with strategic consequences. The problem the U.S. military faces is the renewal of the great power competition with adversaries engaging in multiple domains, thus challenging the traditional definitions of combat, yet also operating beneath the specific threshold warranting military action. This first article in a two-part series will describe the weaponization of social media, the advancement of technology, and how the U.S. can combat this new threat.

NCO Journal provides a forum and publishing opportunity for NCOs, by NCOs, for the open exchange of ideas and information in support of training, education and development.
https://www.armyupress.army.mil/Journals/NCO-Journal/

The Importance

The information domain allows adversaries to engage the U.S. with digital attacks that erode the trust between the military and the American people. The information domain starts at the tactical level, and it is a tactical commander's responsibility to occupy it; however, there is currently a lack of clear guidance on this domain and the aspects of cross-domain warfare. The result is the effect of "paralysis by analysis" and a disregard of social media as a tactical system in the new information domain (Kessler, 2022). Active measures in the realm of social media include coercing others, disinformation, political influence operations in what could be considered the tactical setting for the asymmetric gray zone, hybrid, and next-generation information warfare.

The Operational Environment

Traditionally, basic communication models include sender, receiver, transmission, medium, and message as separate components; however, due to advances in technology, the information domain now includes the internet, radio waves, satellite communications, wireless networks, and social media (Kozloski, 2009; Quain, 2018). For example, when the Islamic State of Iraq and Syria (ISIS) invaded Northern Iraq in 2014, it had approximately 1,500 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 (“Why social media is the new weapon,” 2019). ISIS's online tactics and mastery of the information domain recruited 30,000 fighters from more than 100 countries and spread fear globally.

Military experts are constantly warning service members about social media scams that can affect them and their families. (Department of Defense graphic by Regina Ali)

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 simplicity. ISIS's top recruiter, Junaid Hussein, used the same social media marketing tactics Taylor Swift used to sell her records (“Why social media is the new weapon,” 2019). Also, during the last Mexican elections, one-third of the online conversations were generated by bots.

Social media platforms are addictive by design. Notifications, for example, do not tell the user what a post is about, thus creating a certain level of anxiety, a need for closure, and appealing to emotion. Unfortunately, our young generation of Soldiers is influenced by this type of emotional targeting. Extremist organization recruiters stir negative emotions such as anger to convert young recruits to their cause (“Why social media is the new weapon,” 2019). If units do not occupy the information domain operational environment, they risk enabling other groups to target Soldiers, spread disinformation, and operate with impunity.

Speed and Level of Response

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, 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 those wishing us harm.

The most effective tool against hate and corruption is an educated and empowered Soldier and leader population capable of identifying and discrediting disinformation attempts. The U.S. Army must recognize, at echelon, that social media can be used as a weapon against us; therefore, it must invest in social media literacy and instill awareness of methods and goals of targeted campaigns.

Changes in Technology

U.S. adversaries see social media platforms as potential venues of power ready to be weaponized (Gamberini, 2020). Public health issues such as COVID-19 present an ideal target for social media weaponization due to its divisive and emotional nature. For example, the anti-vaxxer movement promotes a passionate argument that vaccinations are unnecessary and dangerous. The movement is fueled by deep mistrust for authority, thus encouraging misinformation. As a result, diseases such as measles (previously eradicated in the U.S.) have made their most remarkable comeback since 1992. These disinformation campaigns could physically weaken the U.S., as health institutions face a crisis of trust fueled by intentional and unintentional lies (Gamberini, 2020).

Conclusion

Despite 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. military, capable of discrediting disinformation and targeting efforts. Command teams must invest in social media literacy and instill awareness about the methods and goals of targeted disinformation campaigns while measuring the effectiveness of their information campaigns. Despite the arms race between nefarious actors and the tech world, the evolution and education of the human domain is an essential weapon against those who wish the U.S. harm.

The second article of this series will cover strategic communications, command presence and talent management, a detailed threat assessment of dangers to the U.S. in the social media space, and real-world examples of social media incidences under a microscope. ■

References

Fridman, O. (2017). The Danger of Russian Hybrid Warfare. *Cicero Foundation Great Debate Paper, 5*(17). https://www.cicerofoundation.org/wp-content/uploads/Ofer_Fridman_The_Danger_of_Russian_Hybrid_Warfare.pdf

Gamberini, S. J. (2020). Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns. *Joint Force Quarterly, 5*(99).

Kessler, A. (2022). Can social media alter a war? *The Wall Street Journal*. https://www.wsj.com/articles/can-social-media-alter-a-war-nato-russian-bots-colonial-pipeline-national-security-ukraine-cyberwarfare-hack-invasion-11641130267

Kozloski, R. (2009). The information domain as an element of national power. Center for Contemporary Conflict.

Quain, S. (2018). *Traditional communication channels*. Small Business Chronicles. https://smallbusiness.chron.com/traditional-communication-channels-65162.html

Why social media is the new weapon in modern warfare. (2019). The University of Pennsylvania. https://knowledge.wharton.upenn.edu/article/singer-weaponization-social-media/

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, Eqypt. 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.

NCO JOURNAL

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.