Consolidating and Automating Social Media Impacts to Risk

Maj John P. Biszko, USAF

The military has an emerging requirement for software that links two existing types of platforms: those that track blue force movements and those that display social media activity. If this requirement is adequately articulated, funded, and developed, it will represent a major leap forward in force protection, intelligence, and counterintelligence. This short article examines the shared interests of military leaders and social media users and uses an Air Force flight tracking example to illustrate the force protection concerns emerging from this shared interest. It also provides background on mission planning and social media exploitation software suites, articulates a general technical solution to a defined problem, and ends by defining major impact touch points and suggesting future developments.

First, one feature of the military's information environment is a mutually implicative shared interest with social media users all over the world.[1] Military decision makers desire high-fidelity awareness of the location of their forces. Social media users also desire high-fidelity awareness of the location of military forces.[2] As social media users observe aircraft, ships, and land forces, they communicate about those forces.[3] That communication may be speculation about capabilities, the intent behind missions, the will of military decision makers, or perceived opportunities in the operational environment.[4] Since the social media users may also coordinate activities, the actions and reactions of users to an observation of assets or personnel constitute a concern in three major areas. Those areas are (1) force protection, since operational security may be compromised; (2) intelligence, since foreign adversaries may use social media information and platforms to collaborate to one's disadvantage; and (3) counterintelligence, since foreign intelligence and domestic threats may also use social media information and platforms to one's disadvantage.[5]

The flight-tracking of Air Force assets is a sound operational example of this interest convergence and the resultant force protection concerns: A flight takes off and heads toward a sensitive location, and that sensitive location information is shared by an actor on social media, incidentally to the service's relative surprise and disadvantage. Here are three preponderant questions for the Joint Force to process:

1. How does the Joint Force integrate the resulting change in emerging warning intelligence and risk in near real-time?[6]
2. How does the Joint Force do this for all flights automatically without increasing Air Force end strength to ease implementation?[7]
3. In addition to adjusting the risk characterization for risk to the flight mission or risk to Air Force forces, how does the Joint Force adjust the risk for ground and naval forces to compensate for the compromise of Air Force assets' locations by a social media user and make that adjustment using computers at a near-neutral cost?

It is useful to look at blue force tracking and social media exploitation separately and then combine the two after having noted the flight tracking example. First, the Joint Force is generally accustomed to preplanned routes. The data for such routes are stored digitally. While there may be last-minute changes after traditional mission or force deployment planning, the services do, for the most part, store data in advance of a force deployment regarding what the geographic location of the assets or personnel will be at each phase of the mission. The planning cell does not always display the data in that raw a manner: the user sees a flight, voyage, or deployment duration and a route; however, the mission planning software draws from a server that stores roughly at what time the assets or personnel will be over each point in time and space, which is how it is able to generate and display the duration and path.[8]

In addition to planning points in time and space, the services also contract with social media exploitation services for force protection, intelligence, and counterintelligence. In their various versions, the so-called Publicly Available Information (PAI) Toolkits allow military professionals to access social media posts within a user-defined geographic- and time-bounded area. Such toolkits do not actually allow the user to scrape social media in real-time. Instead, contract companies establish user agreements with proprietary social media companies, such as Facebook, Twitter, and the foreign versions of such programs. The contract companies have user agreements that allow them to ingest a certain percentage of data from social media users in a hybrid of cooperatively and noncooperatively accessible PAI. The contract companies then allow the services to buy licenses, which, in turn, allow professionals to search for threats in the proprietary data pool; however, the military user typically manually sets the "target"—the keyword, time boundary, or geographic boundary, which will initiate the simple search. The contract companies providing the licenses usually combine language translation software with their search software, allowing the user to overcome a small part of the socio- or cultural-linguistic barrier.[9]

After describing the problem in broad terms and providing an example, here is a three-part solution:

1. Augment the existing social media access strategy with a collection strategy—meaning that in addition to paying proprietary companies money to allow service professionals to access a limited amount of social media content, the services work with other government agencies to also collect the data from foreign areas or entities—cooperatively or noncooperatively. At this point, the data is not just accessed but also collected, which would necessitate the services working with outside agencies to assign personnel with the appropriate training, certification, mission, and authority to collect.[10]
2. Replicate the data that is accessible through the contract companies, as well as the data that is collected through the appropriate intelligence sources and methods, in a data repository where the coding is compatible with the data from the mission planning and force deployment software suites. The accessed data, which the services pay for, would be siphoned up to a system with a higher classification and stored alongside the collected data.
3. Write the code, and install the corresponding software that would compare the time and geography stamps associated with each social media entry in the main repository with the time and geography stamps of each force movement in the mission planning data set.

For the Air Force operational example, the result would appear thus: a mission planner prepares the flight route. Along with other intelligence injects, he or she receives a preview of the social media landscape surrounding the flight with an emphasis on aircraft recognition or threats. While the software compares the mission planning data with the social media repository data, it would search for any social media post near the planned flight route in the previous five days that references an aircraft or any term indicating an intent to harm. That report would be generated automatically for the mission planner, which the information operations cell would caveat appropriately to compensate for fake or uncorroborated post content.

Second, the program would follow the aircraft in flight while also searching the social media information that is continuously updated in the repository. As it identifies a potential threat indicator, the program would alert intelligence and cyber professionals of either a potential threat indicator or an attempt by an adversary to use bots on social media to deceive the Air Force into altering the flight path—either way, a good insight into grey or red actors' intentions. Third, the program would automatically generate a report on what activity occurred in social

media during the flight, which it assesses, was also potentially related to the flight according to preset parameters, and that social media impact report would be paired with the mission report (MISREP). Both the social media report and the MISREP would be available to the parent combatant command, along with the naval and ground forces reports that the software is generating for other types of force movements.

Such an automation would innovate in several important ways. First, it would begin to allow the services to use social media exploitation software faster than where the speed of human triage is now. Computer software would deliver data-driven analysis. The real limit, paired with artificial intelligence, would become how much foreign user data the Joint Force could realistically access and store, along with how to cope with what would almost surely become a massive denial and deception effort; however, the services are well-armed for tackling such deception using traditional analytic tradecraft. The future would become a game of attempting to corroborate threat information, seemingly apparent in the social media landscape, with other sources and methods, thus driving an even higher-fidelity understanding of enemy capability and intent.

Second, the commander's acceptable level of risk would be much better informed than it is now, since only a minute percentage of all of the social media posts in the world discussing or indicating a threat to US assets and personnel are likely accounted for.[11] Third, data science would allow the services to use the same system to model and predict threat—not just read about it in social media posts.[12] For example, after something happens—after a base attack or an Air Defense Identification Zone penetration—any event of interest—the program can go back in time and freeze what was happening in social media. Thus, after a couple of iterations of the same type of event, the computer can model what the social media landscape typically features right before such an event occurs, thus introducing a pioneer kind of emerging warning intelligence: an unconscientious public warning based in crowd wisdom.[13] ✪

Maj John P. Biszko, USAF

Major Biszko (MACD, Marquette University; MAs, Naval Postgraduate School and American Military University; Certificate of Philosophy, Catholic Distance University; BA, Tulane University) is the director of operations, Air Intelligence Squadron, Air Mobility Command, Scott AFB, Illinois, and a Secretary of the Air Force/International Affairs Middle Eastern Affairs specialist.

Notes

1. Joelle Swart, Chris Peters, and Marcel Broersma, "Sharing and Discussing News in Private Social Media Groups: The Social Function of News and Current Affairs in Location-Based, Work-Oriented and Leisure-Focused Communities," *Digital Journalism 7, no.* 2, (2019): 187–205, https://www.rug.nl/.

2. Danielle K. Kilgo et al., "A New Sensation? An International Exploration of Sensationalism and Social Media Recommendations in Online News Publications," *Journalism* 19, no. 11 (2018): 1497–1516, https://doi.org/.

3. Heather A. Harrison Dinniss, "The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It," *Georgetown Journal of International Affairs* 19 (2018): 43–50, https://muse.jhu.edu/.

4. J. J. Salerno et al., "Issues and Challenges in Higher Level Fusion: Threat/Impact Assessment and Intent Modeling," *2010 13th International Conference on Information Fusion* (July 2010): 1–17.

5. Department of the Air Force, *Air Force Instruction 10-701, Operations Security (OPSEC)* (Washington, DC: Department of the Air Force, 24 July 2019): 1.6, 2.4.5., 6.6.1.1.2, https://fas.org/; Department of the Air Force, *Headquarters Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance, and Cyber Effects Operations Next Generation ISR Dominance Flight Plan 2018—2028* (Washington, DC: Department of the Air Force, 25 July 2018): 15; and Department of the Air Force, *Air Force Instruction 71-101 Volume 4, Counterintelligence* (Washington, DC: Department of the Air Force, 2 July 2019): 3.1, https://fas.org/.

6. DOD, *Joint Publication 2-0, Joint Intelligence* (Washington, DC: DOD, 22 October 2013): I-18, https://www.jcs.mil/.

7. Department of the Air Force, *Draft Program Action Directive D15-03 Implementation of Air Force Cyber Squadrons* (Washington, DC: Department of the Air Force, July 2019): 5.4.

8. Matthew B. Rogers et al., "A Military Logistics Network Planning System," *Military Operations Research* 23, no. 4 (2018): 5–24, https://www.researchgate.net/.

9. John Biszko, Intelligence Exploitation of Social Media (Washington, DC: National Defense Transportation Academy, October 2018), 1–5.

10. DOD, *DoDM 5240.01 Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC: DOD, 8 August 2019), 3.2.c, https://www.esd.whs.mil/.

11. DOD, *CJCSM 3105.01 Joint Risk Analysis* (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, October 2016), B-6, https://www.jcs.mil/.

12. Longbing Cao, "The Data Science Era: The Next Scientific, Technological, and Economic Revolution," *Data Science Thinking* (August 2018): 3–28, https://www.researchgate.net/.

13. James Surowiecki, *The Wisdom of Crowds* (New York: Anchor Books, 2005), 22.