Event Barraging and the Death of Tactical Level Open-Source Intelligence

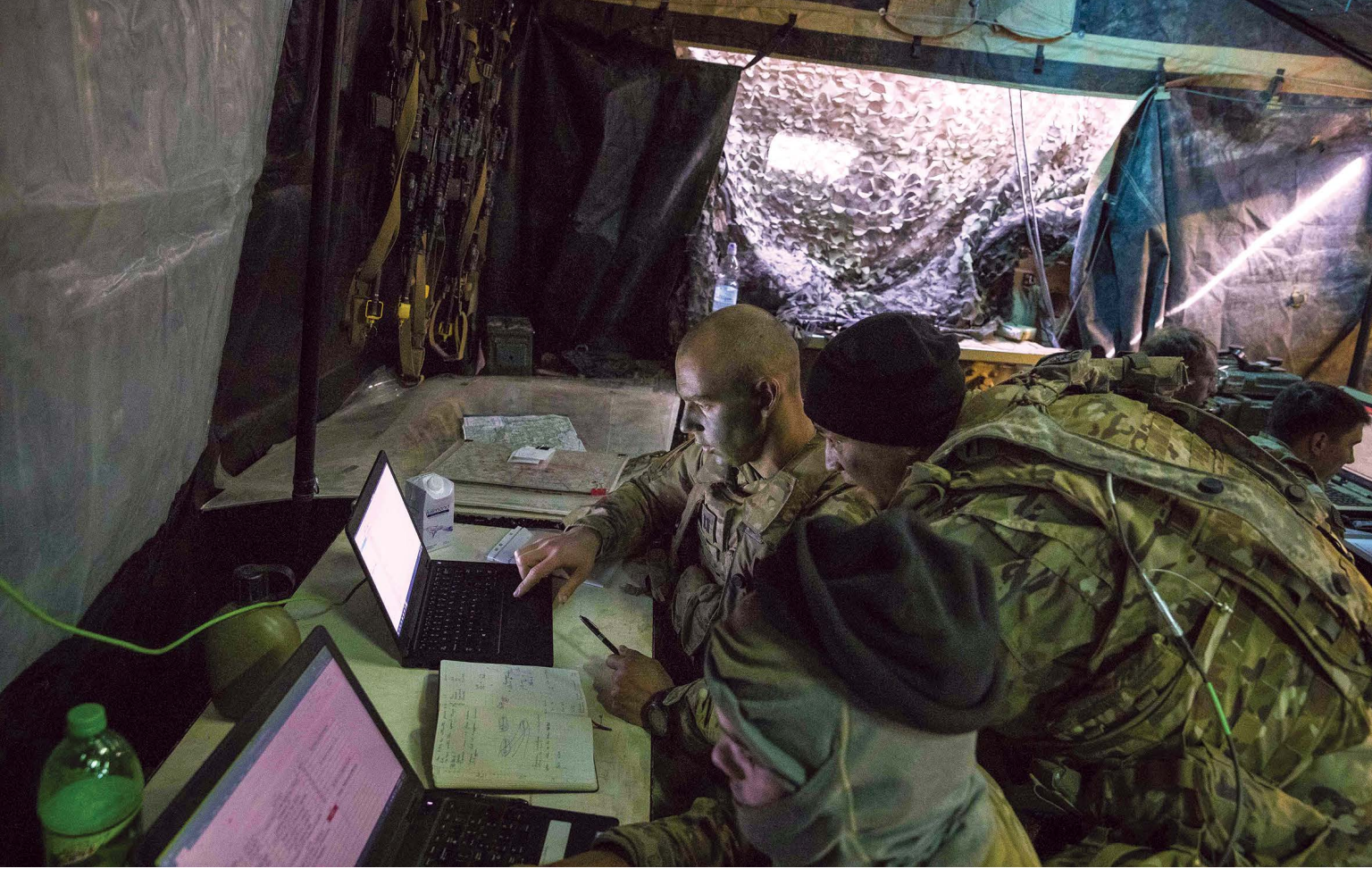
Capt. Michael J. Rasak, U.S. Army

Noncombatants increasingly leverage social media to report on the disposition and composition of military forces, infrastructure status, and the details of ongoing local events, posing a legitimate risk to both friendly and adversarial military activities. Adversarial nation-states and groups have already demonstrated the capability and intent to both mitigate and exploit this phenomenon. In the near future, friendly commanders and analysts will likely endure digital inundation by a series of embellished or entirely fabricated events on social media that directly threaten ongoing or near-term tactical operations, termed "event barraging." In the midst of an event barrage, and due to the immanency of tactical-level operations, commanders are thus compelled to choose from one of two undesirable options: systematically corroborate each event or disregard social media as a platform for observing adversarial activities altogether. The subsequent ramifications of event barraging, trend hijacking, and pinpointed disinformation efforts could then disrupt U.S. decision-making at the tactical level, strain friendly reconnaissance, intelligence, surveillance, and target acquisition (RISTA) assets, and degrade the usefulness of open-source information (OSIF). Nation-states or large groups could incentivize their populations to participate in event barraging, ultimately compromising the integrity of open-source intelligence (OSINT) as a discipline in general.

Capt. Michael J. Rasak, U.S. Army, is the brigade intelligence officer of 4th Cavalry Brigade, First Army Division East. He holds a BA from Michigan State University. His assignments include two deployments to Afghanistan, one as an infantry platoon leader in the 101st Airborne Division (Air Assault) and another as a squadron intelligence officer in 3rd Infantry Division.

Open-Source Intelligence at the Tactical Level

Despite this article's ominous title, OSINT will likely not die as a discipline altogether. The sheer volume of information housed in the open-source domain offers analysts a pool of available data too valuable to cast aside entirely. We need only look at the astute observations of seasoned professionals spanning the entirety of the intelligence community and within the ranks of the military. Lt. Gen. Samuel V. Wilson, former Defense Intelligence Agency director, claims OSINT provides roughly 90 percent of the information used by the intelligence community.[1] Robert Cardillo, National Geospatial-Intelligence Agency director, argued that "unclassified information should no longer be seen as supplemental to classified sources, but rather it should be the other way around."[2] Even those without a vested interest in the security of the nation, like Vice News, have remarked on the boundless swath of valuable military information to be gleaned from publicly available sources.[3] The pool of available OSIF manifesting from the rise of social media has only encouraged further excitement: geotagging, georeferencing, web scraping, sentiment analysis, and lexical analysis are a few emerging technologies and techniques. OSINT offers commanders from the tactical to the strategic levels invaluable insight deep into nonpermissive environments,

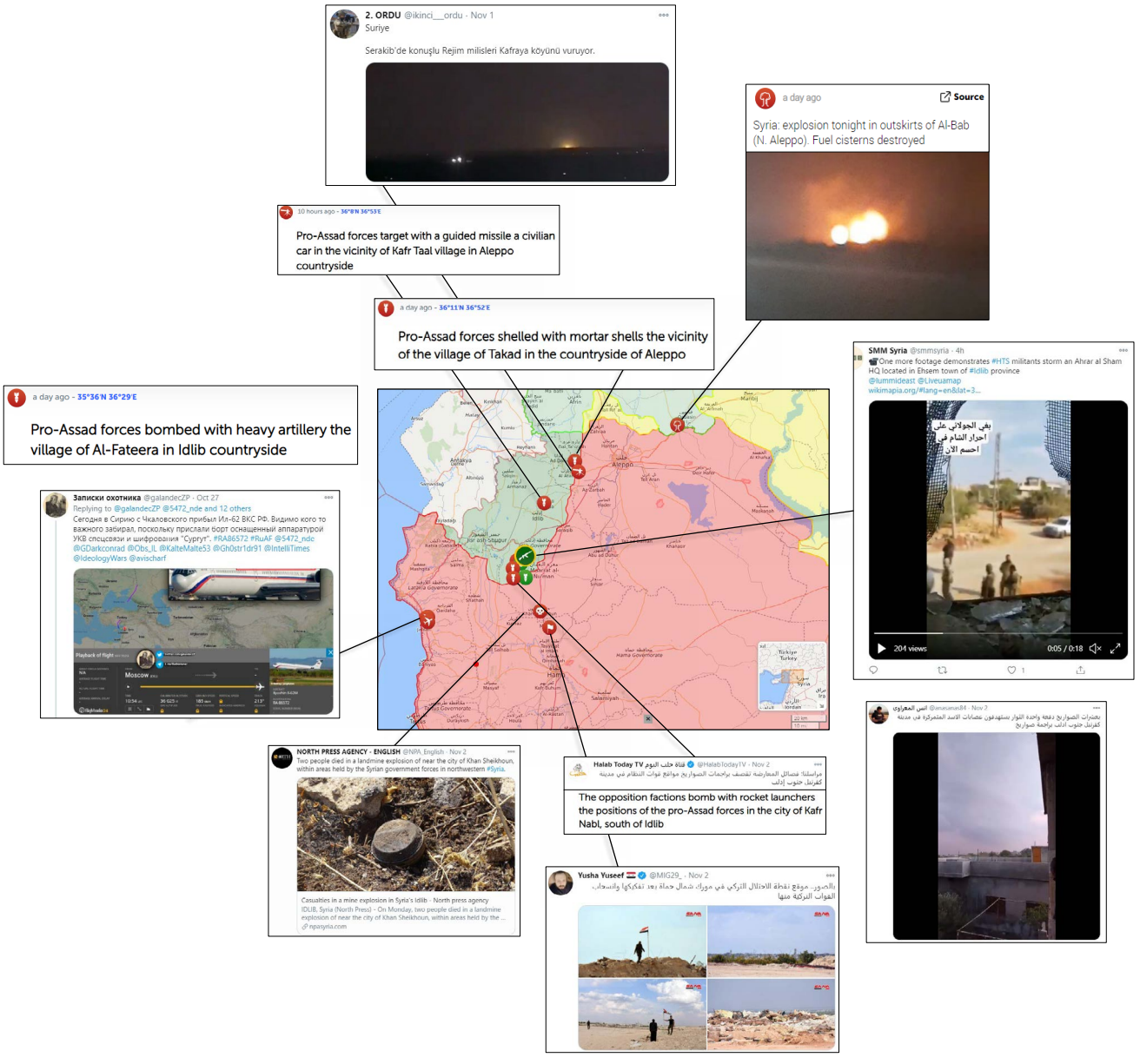


Warrant Officer Alan Mendoza (*right*), an all-source intelligence technician assigned to 2nd Battalion, 34th Armored Regiment, 1st Armored Brigade Combat Team, assists Capt. Kenneth Russel, the battalion intelligence officer, 8 April 2019 during exercise Allied Spirit X in Hohenfels, Germany. (Photo by Sgt. Thomas Mort, U.S. Army)

which were previously obtained only through clandestine efforts. Armed with this higher resolution, commanders are better able to understand and visualize the battlefield, thus offering them an advantage when they must describe, direct, lead, and assess operations.

At the tactical level, OSINT offers ground force commanders near-real-time information critical to decision-making. Social media especially provides analysts the opportunity to rapidly collect, monitor, and assess events within a commander's area of operations. Countless ordinary citizens armed with smartphones, internal GPS devices, and Twitter accounts unwittingly divulge insight into the disposition, composition, and strength of enemy forces, the status of infrastructure, ongoing events, and the general sentiment of the population. Moreover, the inherent immanency of tactical level operations (as opposed to operational- or strategic-level operations) renders information gleaned from OSINT collection of even greater importance. Take, for instance, an infantry platoon out on patrol, operating only several kilometers from a village. When a battalion or brigade intelligence officer observes a large volume of tweets indicating enemy fighters have massed in the village, that officer has an obligation to corroborate the information to the greatest extent possible and disseminate it to the platoon leader on the ground. Failure to do so could result in the platoon becoming ambushed or in a missed opportunity to engage the enemy under more advantageous conditions.

Scholars, military professionals, and members of the intelligence community have all remarked on the effectiveness of OSINT at the tactical level. In "Operationalizing OSINT Full-Spectrum Military Operations," Senior Chief Petty Officer Ron Penninger authored a fantastic example of just how effective OSINT at the tactical level is, and how sentiment analysis and georeferencing can directly contribute to the decision-making of ground force commanders.[4] RAND Corporation, too, has commented on the



(Figure created by author with screenshots taken from Live Universal Awareness Map)

Figure 1. Live Universal Awareness Map Example: Syria, 3 November 2020

paradigm-shifting effects of "second-generation OSINT." Heather J. Williams and Ilana Blum argue, "Analysts … can use a combination of Google Maps, Wikimapia, publicly available tweets, Facebook posts, and YouTube videos to pinpoint exact locations of ongoing military actions."[5]

Leveraging OSINT for tactical application goes well beyond mere rhetoric or lip service; militaries, government agencies, nongovernmental organizations, and corporations are capitalizing on it right now. Live Universal Awareness Map (Liveuamap) serves as perhaps one of the greatest examples. On its website, Liveuamap explains it is an "independent global news and information site," which aims to assist individuals in "making conscious decisions about their security."[6] Drawing primarily from social media posts, the site provides near-real-time information on the movement of military personnel and

equipment, civil unrest, violence, and other activities, and overlays these events on an interactive map (see figure 1, page 50). For example, at the time of this writing, one of the most recent events in Libya (crowdsourced from Twitter) indicates, "[six] anti-aircraft Russian-made Pantsyr vehicles arrived in Sirte."[7]

Hong Kong protesters using "HKMap Live" during the massive demonstrations of late 2019 and early 2020 offer another clear example of how effective untrained noncombatants can be at tracking the movement of government forces. Through crowdsourcing and social media, protesters tracked the composition and disposition of police forces, communicated intent, and massed manpower at times and places of their choosing. Hong Kong protesters declared their tracking efforts were used to avoid police forces, whereas the Chinese government declared that protester efforts were used to facilitate the ambushing of police forces. Regardless of which argument held greater truth, social media clearly facilitated the execution of tactical doctrine—that is, gain and maintain contact, break contact, or conduct an ambush.

Militaries across the globe are increasingly leveraging social media as the first step in the targeting process—that is, to "find" or "detect" what will eventually be "finished" or "engaged." As explained by Williams and Blum, "many all-source analysts start with OSINT and then layer on classified source material" and in this way, rapidly decrease the time and energy it takes to facilitate targeting operations.[8] Battalions, brigades, and divisions would be remiss to refrain from displaying pertinent social media feeds adjacent to their maps on the walls of their command posts; the situational awareness OSIF provides in the modern era is just too important to disregard. The battlefield has become an environment where eyes and ears are everywhere, for friend and adversary alike to consume and use as they please. It seems at least one of the characteristics of the offense has been utterly trounced: surprise.

Understanding that "every citizen is now a sensor" raises the question, "How this can be mitigated?" Or, flipping the question around, "How this can be weaponized?" The rest of this article will explore these questions and address some of their implications.

Event Barraging

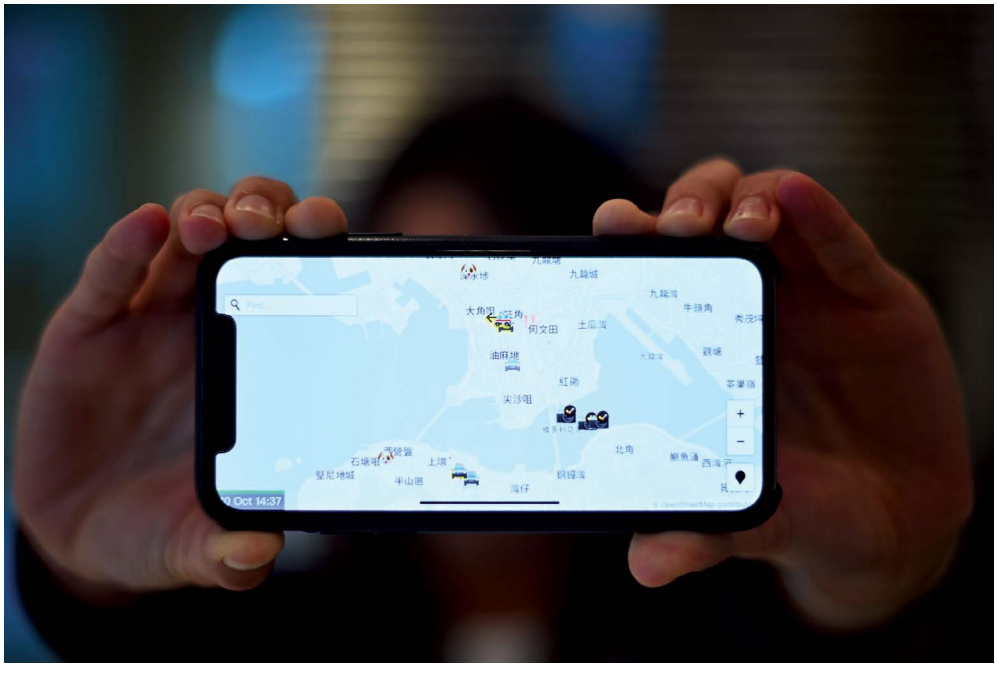
Trained OSINT practitioners are advised to question the authenticity and credibility of social media OSIF due to the prevalence of deception and bias. But how exactly does a practitioner verify credibility and authenticity of a Twitter post? The usual answer is to corroborate this information with information from at least one other intelligence discipline and subsequently convert the information from questionable single-source raw data to a veracious multi-source finished analytical product. While this process is the gold standard, it can be cumbersome or difficult—especially when analysts are supporting the rapid tempo of tactical-level operations. Often, analysts rely on corroboration through multiple collection attempts from the same (or similar) sensor. An example of this outside of OSINT could be using two separate human intelligence sources to corroborate a piece of information, or the use of two separate unmanned aircraft system full-motion video feeds to corroborate a piece of information.

OSINT practitioners often can and do rely on aggregating OSIF from many sources to do a similar process. Williams and Blum explain that "[a] single Twitter tweet reflecting a random individual's view on the Islamic State of Iraq and al-Sham (ISIS) is of almost no intelligence value; however, synthesizing all the tweets on views of ISIS within a geographic area is of great intelligence value."[9] Penninger offers another example by recommending a web scrape of a geographic area (in this case, a village) prior to a mission to determine the population's baseline sentiment—and observing the changes in sentiment as U.S. forces execute their operation. In this case, he argues, changes in the village sentiment can help ground force commanders to "make informed decisions" and "shape their acts to best attain the result intended by higher command."[10]

With the increasing use of bots (automated programs), artificial intelligence, and machine learning comes the potential for adversaries to completely fabricate, artificially inflate, or mask existing trends, patterns, ideas, events, or actions. Jarred Prier's "Commanding the Trend" outlines the increasing sophistication and effectiveness of "trend hijacking" on social media. He explains that "bot accounts are non-human accounts that automatically tweet and retweet based on a set of programmed rules," which subsequently inflate a given narrative (see figure 2, page 53, for an example).[11] He further notes that as of 2017, Twitter estimated nearly 15 percent of its accounts were bot accounts.[12] Individuals, groups, or entire nation-states can commit their resources to trend hijacking for whatever purpose they desire. For instance, one white supremacist group in June 2020 announced its initiation of Project

SOCH (Solar Orbiting Casaba Howitzer), which aims to build "an automation system … able to rapidly generate social media accounts with the click of a button, making it easier … to maintain a presence on heavily censored platforms."[13] While scholars like Prier delve into the national and strategic implications of trend hijacking, the same concerns can also filter down to the tactical level.

Beyond bots, adversaries may also leverage GPS spoofing to generate false geotags associated with their social media posts. Not only are nation-states or sophisticated groups capable of GPS spoofing but everyday noncombatants can also do the same thing. Commercially available apps like "Fake GPS Location–GPS Joystick" allow anybody to override the internal GPS systems in their smartphones with just a little bit of effort. GPS spoofing can also be organized and directed at designated locations. Janus Rose explains that a group in 2016 "scann[ed] and sampl[ed] the profiles of 60 nearby Wi-Fi networks …, re-broadcast[ed] those networks," and accordingly, enabled anybody with access to the internet to trick their phones into thinking they were located at the Ecuadorian Embassy.[14] Thus, adversaries are not only armed with the ability to fabricate fake events but also to direct those events at designated geographic regions.



After Beijing stepped up pressure on foreign companies deemed to be providing support to the pro-democracy movement in Hong Kong, Apple removed the "HKmap.live" app 10 October 2019 because it was allowing protesters in Hong Kong to track police movement. (Photo illustration by Philip Fong, Agence France-Presse)

In revisiting our infantry platoon operating nearby in a village, it is then feasible that an adversary could artificially inflate or outright fabricate a trend or "event" that indicates to an unsuspecting analyst there is an emerging threat in proximity. If our analyst supporting that infantry platoon geofenced his or her search parameters to roughly match the borders of the village, then perhaps only dozens of tweets and retweets could fundamentally shift the sentiment or ostensible threat resident within the village. If our analyst is unable to corroborate the emerging threat with a separate intelligence discipline, then he or she must rely on the aggregated OSIF from social media and generate an OSINT report for the ground force commander. The commander is then left with three choices: request RISTA support from higher headquarters, redirect his or her own sensors, or simply rely on the intelligence he or she has been handed and react accordingly.

While the severity of this instance may seem relatively benign (or just another example of the "white noise" analysts are all too familiar with) then expanding this problem set to its next natural evolution raises some serious concerns. Imagine our analyst sees three emerging events: fighters have massed in the village to the east, a mortar team has established itself four kilometers to the west, and the bridge required for egress to the south has been destroyed. Well, now there are three events the analyst, higher headquarters, and the ground force commander must confirm. Three new named areas of interest and intelligence requirements have just developed, three new events need to be corroborated through separate RISTA assets, and the ground force commander must make a

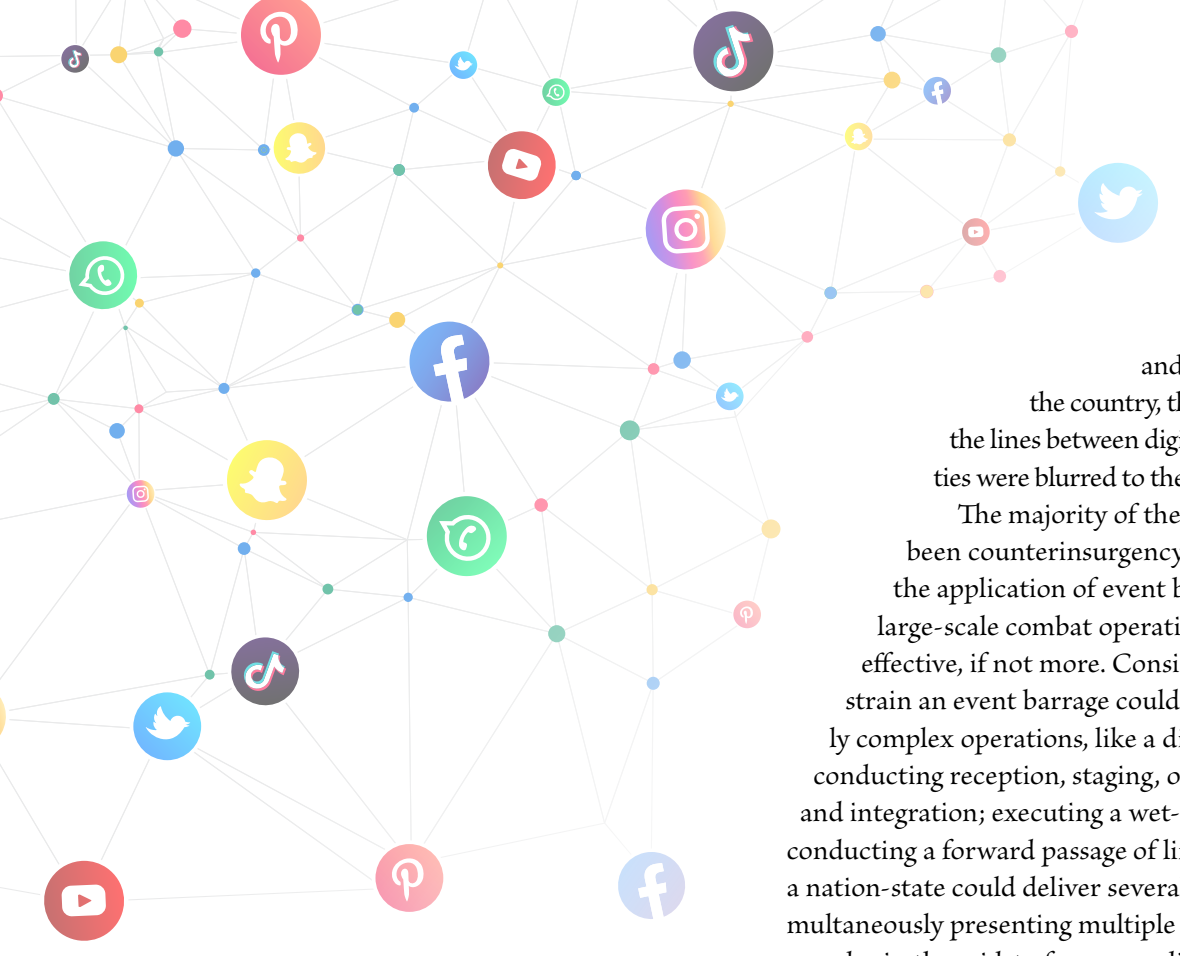
decision on his or her next action. Now raise the number of events from three to ten. This method of inundating a ground force with OSIF trends over social media can be called event barraging. If we assume available RISTA assets will be redirected to answer these emerging intelligence requirements, then we must remember these RISTA assets have also been pulled away from whatever mission they were originally tasked to do, which was likely to collect on priority intelligence requirements that had genuine merit. Event barraging can then be used as a means to place incredible strain on available RISTA assets, disrupt collection plans, and mask genuine intelligence feeds. In this vein, event barraging can be seen as a means of nonlethal fires, deliberately hindering the decision cycle of commanders, and intended to disrupt tactical operations at worst and neutralize operations at best.

(Screenshot by author via Twitter)

Figure 2. Example of a Botnet on Twitter

A frustrated analyst or commander who altogether dismisses the information during an event barrage could generate even greater problems. As addressed in the first part of this article, OSIF and social media offer analysts and commanders an incredible advantage in the field. Militaries are increasingly incapable of maneuvering throughout the battlefield without being observed and reported on by everyday citizens. Moreover, if we consider that there are still *actual* people *genuinely* reporting on the movement of personnel—even in the midst of an event barrage—then one (or more) of the emerging events may be genuinely true. And if we assume the event barrage is comprised of all high-priority or imminent events, then the ground force and supporting analysts are thus *required* to corroborate everything they see to determine exactly which events are true.

An adversary could deliver event barrages to do more than just disrupt ongoing U.S. operations. They could be used to mask adversary movement, prevent U.S. forces from entering an area, complicate target validation, disrupt ground lines of communication, lure U.S. forces into an area, or augment in adversarial engagement area development. This is especially true if adversaries take even the most marginal steps to supplement the ongoing event barrage outside of social media through the use of computer-generated videos, deepfakes, fabricated gray literature or media reports, or staged small physical or electronic evidence that could lead to false corroboration. For instance, if an adversary wished to disrupt ground lines of communication, the adversary could event barrage the desired area



and have a single actor disturb the earth at that location (to replicate an improvised explosive device emplacement), ultimately deceiving imagery analysis. Civil unrest barrages could be falsely corroborated through repurposed (or computer-generated) videos and several sets of burning tires. Massing fighters could be falsely corroborated through one person with a radio relaying incorrect information over the net to deceive communication analysis. While these examples are overly simple, the fact remains that event barraging has the potential to turn initial deception efforts from single-source one-off reports to legitimately authentic-looking multisource reports.

As an example of falsely corroborating civil unrest events, consider the confusion circling the June 2020 Capitol Hill Autonomous Zone in Seattle. Beyond the opposing narratives spun in the social media underworld, reporting "on-the-ground facts," mainstream media outlets themselves fell victim (or deliberately contributed) to the chaos. For instance, Fox News displayed an image of armed guards occupying the area but removed the image shortly after the *Seattle Times* noted the image was of an entirely separate event that took place in Minnesota. While Fox News claimed the photo was part of a "collage" that "did not clearly delineate" images from Seattle and other events across the country, the fact remains that the lines between digital and physical realities were blurred to the point of obscurity.[15]

The majority of these examples have been counterinsurgency oriented, but the application of event barraging during large-scale combat operations could be just as effective, if not more. Consider the additional strain an event barrage could add to already highly complex operations, like a division or brigade conducting reception, staging, onward movement, and integration; executing a wet-gap crossing; or conducting a forward passage of lines. In these cases, a nation-state could deliver several event barrages, simultaneously presenting multiple dilemmas to a commander in the midst of commanding and controlling an already multifaceted operation. A forward-thinking group or nation-state could even have multiple event barrages (and their supplemental measures) prefabricated and loaded for delivery at key times or places. Event barrages could be manufactured days, weeks, or months in advance. Humanitarian crises, broken dams, civil disturbances, destroyed bridges, and fake armored brigades could virtually pepper the battlefield, straining available RISTA assets and diverting U.S. reconnaissance efforts away from genuine targets. "Rolling" event barrages could increasingly divert U.S. attention further and further from genuine objectives, and the enemy would only have to make an occasional event barrage true to compel U.S. focus.

Paramount to delivering an effective event barrage is obtaining the participation of as many disparate cyber actors as possible. While a bot army controlled by a handful of individuals has the potential to fabricate and/or inflate a given event, currently employed techniques and technologies can usually identify and thus eliminate or disregard a particularly inauthentic-looking event or trend. Advanced lexical analysis, keyness analysis,

Graphic elements by myriammira and starline via Freepik, www.freepik.com. Composite graphic by Arin Burgess, Army University Press

and frequency profiling can be used to attribute written text to a specific demographic, group, or even to a single author.[16] For instance, if an initial body of tweets or articles commenting on an emerging humanitarian crisis embodies the hallmark writing characteristics of a known nefarious group, this event can be disregarded as a mere disinformation attempt. However, if the event gains traction across the larger global audience and thousands of people comment, post, or contribute their own unique text or images to the discussion, more energy and time must be committed to sift through what is real and what is fake. Consider the 2020 #DCblackout trend on Twitter; started by just three followers, the hashtag exploded within hours despite Twitter's attempts at halting the misinformation campaign. Half a million people retweeted the event and a large portion of the country believed the government shut down the local internet to suppress civil unrest.[17] Though the illegitimacy of #DCblackout was eventually exposed, the initial confusion of the event serves as a compelling example of the potentially disruptive effects an event barrage can have on streamlined and rapid tactical operations.

The potential for event barraging to become adversarial doctrine should not be underestimated. Though not labeled an event barrage, perhaps the first form of this tactic in its infancy manifested in 2014 Ukraine. While the analysis of events in Ukraine have been comprehensively covered by political and strategic thinkers across the globe, it is worth noting several key highlights. Russia exhibited the capability of barraging Ukrainian protests in 2014 with "a network of dozens of social media groups … used to spread fake rumors to undermine the Ukrainian troops or discredit army leadership."[18] Ukrainian soldiers themselves were directly targeted with "Short Message Service [SMS] messages, coming to their cell phones most likely from Russian electronic warfare systems."[19] Lastly, Russian actors utilized simple methods like "bikini trolls" sporting profile pictures of attractive women to gain digital followership and defeat "some of the tools for troll and bot analysis."[20] These characteristics of digitally delivering informational events, targeting specific locations and people, and countering analytical deception-seeking tools are indicators of a growing doctrine that could be marshaled at a tactical level.

Another consideration we should take into account is the cost-benefit analysis of performing an event barrage. Is the efficacy of an event barrage worth the cost of resourcing, organizing, and delivering it? This question is perhaps best framed by comparing the cost-benefit analysis to other types of obstacles, nonlethal and lethal fires, and military deception efforts. To begin with, as outlined by Penninger, Mikhail Burchik's Internet Research Agency, a Russian company directly responsible for ongoing disinformation campaigns in the United States, operated on a budget measured in the "single digit millions of dollars for a couple of years of harassment and disruption."[21] Moreover, RAND notes that at Russia's Saint Petersburg troll factory, "employees are paid at least US$500 per month to manage fake accounts, spreading propaganda and disinformation."[22] Combining these figures, it seems logical a team of fifty or so dedicated Russian cyber actors could launch a continuous, comprehensive disinformation campaign for somewhere around $40,000 per month. We must also remember this expense includes the cost of purchasing advertisements and running myriad servers and associated botnets. Therefore, the cost of one month of operations from this relatively small cohort would equal just shy of one-half of a single hellfire missile, around forty unguided howitzer shells, or four hundred rounds of 30mm ammunition delivered from an AH-64 Apache. Or, the cost of an entire month's worth of event barraging could equate to only ten hours of flight time for a single MQ-1B Predator.[23]

Delivering an event barrage is a cheap, accurate, and rapid way to disrupt U.S. tactical decision-making, strain RISTA resources, generate advantageous battlefield effects, and degrade the value of available OSIF. Generating and delivering an event barrage is certainly within the capability of most modern nation-states, many adversarial groups, and perhaps even lone-wolf cyber actors armed with formidable bot armies.

The Death of Tactical Level OSINT

The consequences of event barraging, misinformation campaigns, trend hijacking, and military deception will fundamentally detract from the usefulness of OSINT at the tactical level. Information on the internet is not an abstract independent entity, relatively malleable but still capable of holding its true form despite the repeated efforts of interconnected users to continuously poke, prod, and manipulate it. Rather, information on the internet *is* the interconnected users who inhabit that domain, and its content manifests based on the will and power of those users. As the internet grows and expands,

so too will the capabilities of nation-states and actors to change it. Like the infantry platoon by the village, information gleaned from the internet will be questioned to the point where it becomes virtually useless. Rather than answering information requirements, OSIF will simply serve to generate *more* information requirements. Is there really a riot going on in Kabul? Did the enemy really just relocate one of its Panstir batteries? Is the bridge along my egress route actually destroyed?

It may not even be too far to surmise that nation-states will consider it a *duty* for citizens to deluge the internet with false information. Opposite of the twentieth-century war slogan "loose lips sink ships," we could potentially witness a world where governments encourage citizens to flood the digital domain with false information. Not only would this serve to protect the livelihood of deployed soldiers and/or disrupt enemy plans, but it could also be carried out by every citizen with a smartphone and access to the internet, no matter how far geographically separated from the fighting. In fact, governments could even offer monetized or civil incentives to drive citizens to carry out disinformation campaigns, perhaps in the form of tax breaks or citizenship medals. The larger the number of people who contribute to event barraging and disinformation, the greater the likelihood of success. One million different people posting, tweeting, retweeting, and writing will defeat mechanisms intended to identify online disinformation campaigns, like lexical analysis, network analysis, or geospatial analysis. Indeed, the "whole-of-nation" approach to warfare could certainly encourage the marshaling and weaponization of open-source information to levels never seen before.

Recommendations

Several options are available when looking at how to overcome the detrimental impacts of event barraging, trend hijacking, and pinpointed disinformation campaigns, though none are ideal on their own: (1) as a nation, continue to commit resources and energy into developing better analytical tools and processes to cope with increasing disinformation on the internet; (2) reign in our reliance on social media as a means of battle-tracking adversarial activities; and (3) aggressively target adversarial botnets, troll factories, and known nefarious actors during global and theater shaping activities. By blending all three efforts, we could see a reduction in risk to our force and mission and potentially safeguard the usefulness of OSIF.

Developing ever-more sophisticated tools to cope with emerging cyber threats has been an American defense policy since the dawn of the computer age.[24] We could potentially benefit, however, from revisiting simple processes and procedures. For instance, registering all the significant botnets, cyber adversaries, and their associated digital fingerprints, consolidating that information in a centralized and filterable location, and disseminating that information down to tactical-level analysts for rapid cross-referencing could help alleviate the implications of weaponized OSIF.[25] In 2017, RAND noted the need for brigade combat teams to augment their defensive and offensive cyber capabilities, in part due to brigade commanders' need "to respond with sufficient speed to such events in what is likely to be a dynamic, information-rich environment."[26] Certainly enduring a nonlethal cyberattack like an event barrage counts as one of these instances and would be at least partially mitigated from the synchronization or integration of cyber and intelligence professionals at the tactical level. Moreover, standardizing and enforcing OSINT training for tactical-level analysts would enable the spread of best practices and lessons learned, and it would inform all involved parties of emerging threats and trends. While conventional military procedures prohibit the practice of OSINT among nontrained analysts, it would be naïve to assume analysts utterly disregard OSIF altogether, especially as a greater percent of the world's population deliberately reports on the adversary's activities. And even if all-source analysts refrain from overtly incorporating OSIF into their assessments, their exposure to information on social media will likely contribute to forms of bias or inherently flawed analysis.

In addition to increased training, streamlined information sharing, and the integration of cyber experts at the tactical level, we should also be certain to approach OSIF with even greater caution than previously practiced. With the adversary's increasing use of botnets and trend hijacking, aggregating OSIF from small sample sizes could pose legitimate concerns for skewed results and could consequently enable the adversary to manipulate or forecast future U.S. military actions. Information gleaned from a small geofenced or demographic-fenced sample size should always be treated with a high level of skepticism, and the need for corroboration from intelligence disciplines outside of OSINT should be prioritized. Unfortunately, many U.S. adversaries acknowledge this

very fact, which is currently prompting countries like China and Russia to develop and institute their own national intranet or highly censor information coming into their country from the global internet.[27]

Lastly, targeting adversarial entities responsible for carrying out event barrages and disinformation campaigns should be one of the top U.S. priorities during the shaping and deterring phases of any military operation that anticipates "boots on the ground." Though targeting nefarious cyber actors is far from an innovative concept, it is important to note exactly how difficult this would be to achieve with efficacy, especially when we consider the ease in which something like an event barrage could be rapidly projected across the globe. For instance, botnet controllers in Russia could, and likely will, deliver pinpointed disinformation campaigns in support of ground operations in proxy wars they are not overtly involved in. Moreover, the difficulties in overcoming international legal and political boundaries between nation-states could pose a serious problem in the targeting of actors resident within other sovereign nations. As we have seen throughout the last several decades, merely attributing an actor or actors to a single cyberattack is difficult enough, let alone following through with a retaliatory or preemptive targeting effort. We owe it, however, to those commanders responsible for the well-being of their soldiers and the security of the Nation to develop and implement mechanisms to overcome these obstacles. ■

Notes

1. Libor Benes, "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm," *Journal of Strategic Security* 6, no. S3 (2013): S24, http://dx.doi.org/10.5038/1944-0472.6.3S.3.

2. Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), 3, accessed 22 October 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

3. Ben Sullivan, "Twitter's the Only Tool You Need for Tracking the Military," Vice News, 24 April 2017, accessed 22 October 2020, https://www.vice.com/en/article/wn3g99/twitters-the-only-tool-you-need-for-tracking-the-military.

4. Ron Penninger, "Operationalizing OSINT Full-Spectrum Military Operations," Small Wars Journal, 14 January 2019, accessed 22 October 2020, https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations.

5. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 34.

6. "About," Live Universal Awareness Map, accessed 22 October 2020, https://usa.liveuamap.com/about#history.

7. "Libya," Live Universal Awareness Map, accessed 22 October 2020, https://libya.liveuamap.com/en/2020/26-june-6-antiaircraft-russianmade-pantsyr-vehicles-arrived.

8. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 37.

9. Ibid., 10.

10. Penninger, "Operationalizing OSINT."

11. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (2017): 54, accessed 22 October 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

12. Ibid.

13. "White Racially Motivated Violent Extremists Developing Program to Create Bulk Social Media Accounts," Open Source Intelligence Bulletin 20-06-59 (Orlando, FL: Central Florida Intelligence Exchange, 25 June 2020).

14. Janus Rose, "Spoofing Tool Lets You Catch Pokémon from Julian Assange's Embassy Prison," Vice News, 19 July 2016, accessed 22 October 2020, https://www.vice.com/en/article/53d5pk/skylift.

15. Jesse Drucker, "Fox News Removes a Digitally Altered Image of Seattle Protests," *New York Times* (website), 23 June 2020, accessed 22 October 2020, https://www.nytimes.com/2020/06/13/business/media/fox-news-george-floyd-protests-seattle.html.

16. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 24–25.

17. Kate O'Flaherty, "Twitter Suspends Accounts Posting about DC Blackout for Spreading 'Misinformation,'" *Forbes* (website), 2 June 2020, accessed 22 October 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/06/02/twitter-suspends-accounts-posting-about-dc-blackout-for-spreading-misinformation/#4375b9f8530d.

18. Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corporation, 2018), 16.

19. Ibid.

20. Ibid., 23.

21. Penninger, "Operationalizing OSINT."

22. Helmus et al., *Russian Social Media Influence*, 22.

23. Mark Thompson, "Costly Flight Hours," *Time* (website), 2 April 2013, accessed 22 October 2020, https://nation.time.com/2013/04/02/costly-flight-hours/.

24. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 12–13.

25. "Spamhaus Botnet Controller List," Spamhaus, accessed 3 November 2020, https://www.spamhaus.org/bcl/. See the Botnet Controller List as an example of an approach to consolidate and rapidly disseminate large quantities of known botnets.

26. Isaac R. Porche III et al., "Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below" (Santa Monica, CA: RAND Corporation, 2017), 2.

27. Jane Wakefield, "Russia 'Successfully Tests' Its Unplugged Internet," BBC News, 24 December 2019, accessed 22 October 2020, https://www.bbc.com/news/technology-50902496.