It’s Time for Cavalry to Get Serious about Cyber Reconnaissance

by COL Curt Taylor

On Feb. 23, 2015, Bato Dambeyez did something entirely unremarkable for a young man of his generation. He posted a picture of himself standing in his military uniform, weapon in hand, on social media. What made this post remarkable, even historic, was the fact that Dambeyez was a member of the Russian 37th Motorized Infantry Brigade based in Buryatia, Siberia, and the photo was taken inside the Donetsk region of Ukraine, more than 3,000 miles from his hometown.[1] This photo, along with others, provided clear and convincing evidence to a global audience that Russian conventional forces had invaded the sovereign territory of Ukraine.

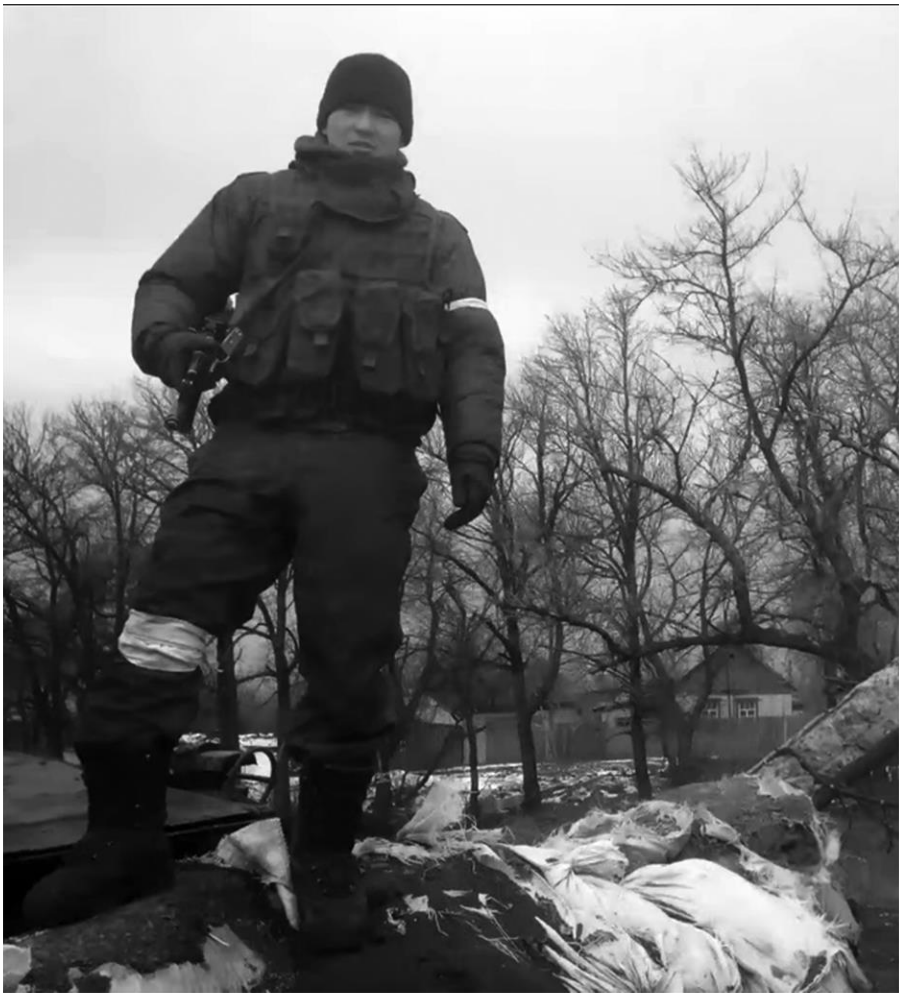

Figure 1. A Russian soldier’s post on social media following the invasion of Ukraine. *(Photo accessed at https://www.vox.com/2015/6/17/8795235/russia-ukraine-troops)*

In July 2014, John Reed, the Jerusalem Bureau chief for ***Financial Times***, tweeted that he was observing the insurgent group Hamas firing rockets from a location near the al-Shifa hospital in Gaza. He was immediately met with a torrent of threats on social media accusing him of providing vital tactical intelligence to the Israeli military.[2]

In August 2017, 1st Brigade Combat Team (BCT), 4th Infantry Division, was conducting a reconnaissance-in-force at the National Training Center (NTC) when two lieutenants manning a provisional “cyber-recon team” reported two critical pieces of enemy information to the brigade. An opposing-force (OPFOR) augmentee Marine Corps company was defending a critical chokepoint along the brigade's axis of advance, and an OPFOR artillery battery was operating from a firing point south of the Tiefort Mountain Range. Based on this information alone, the brigade redirected its lead battalion to avoid the ambush in restricted terrain and fired a pre-emptive rocket mission to destroy the OPFOR battery. What made this action remarkable was the fact that the cyber-recon team had acquired this information, including real-time location data, entirely through collection of open-source information gained through Facebook, Snapchat and Tinder.[3]

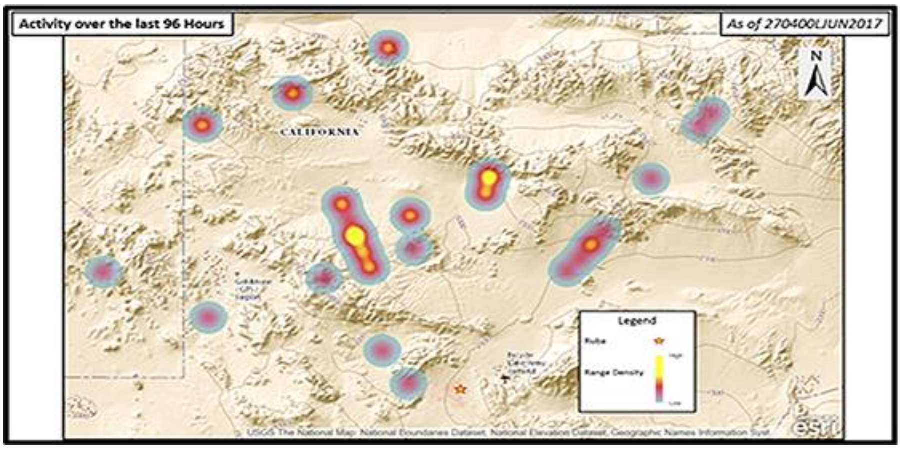
Activity over the last 96 Hours
As of 270400LJUN2017
N
CALIFORNIA
Legend
Rube
Range Density
High
Low
USGS The National Map: National Boundaries Dataset, National Elevation Dataset, Geographic Names Information Syst.
esri

Figure 2. This heat map, produced by the 1/4 BCT cyber-recon team, shows the best estimate of OPFOR locations during an NTC rotation based entirely on social-media trolling. This estimate was surprisingly consistent with templated OPFOR locations derived from other sources.

These three incidents suggest that something fundamental is changing in the way information moves on the battlefield. In all three cases, actors in an ongoing conflict provided real-time, actionable tactical intelligence to a global audience. Collecting this real-time tactical information on the battlefield has long been the province of the cavalry scout. As this information gradually migrates from the land into the cyber domain, it may be time for the U.S. Army to reframe its very idea of what it means to do reconnaissance.

The Duke of Wellington famously quipped that "the whole art of war consists of understanding what is on the other side of the hill."[4] For centuries, achieving that understanding has required commanders to put young Soldiers on the ground, under conditions of great danger, to peer over to the other side of that hill. Successful militaries have constructed elaborate, purpose-built reconnaissance organizations that are uniquely trained and equipped to accomplish this purpose. These formations advance forward of the main body and employ the tools of both ground and air reconnaissance to fight for the information vital to effective battlefield decision-making.

While that requirement will certainly endure in the 21st Century, the growing ubiquity of digital sensors and diffusion of the tools of mass media suggest a new challenge. In this new world, much of the information essential to effective tactical decision-making may appear in cyberspace long before it is extracted through the dangerous and painstaking process of air and ground reconnaissance. Such an important shift requires a reframing of our traditional approach to reconnaissance. Is it now necessary to expand the concept of military reconnaissance to include the cyber domain? If so, how should such a capability be organized in the U.S. military? Who should do it and what are the hazards with such an approach?

This article will investigate the feasibility and limitations of cyber reconnaissance as a military concept. The investigation will demonstrate that the U.S. Army would gain an important competitive advantage in the coming decades by expanding the mission of its reconnaissance units into the cyber domain:

- The article will do this by first reviewing the Army's current reconnaissance doctrine and comparing it with the concept of "cross-domain maneuver" as outlined in the Army's future warfighting concept.[5]
- Second, this article will examine recent cases of military conflict in digitally empowered societies to identify emerging patterns that may suggest important changes in the character of future conflict.

- Third, this article will review several important tools already available on the commercial market that would provide a clear competitive advantage today.
- Fourth and finally, this article will review the perils of expanding military operations into the cyber domain, the potential effects on personal privacy and the blurring of the line between military and personal risk.

Reconnaissance in multi-domain battle

Current U.S. Army doctrine defines the purpose of battlefield reconnaissance to “help commanders cope with uncertainty, make contact under favorable conditions, identify opportunities, prevent surprise and make timely decisions.”[6] Historically these missions have fallen to cavalry units because of their superior mobility and agility.

Before the advent of motorized technology, the horse provided this essential mobility differential over the foot-bound infantryman. In the 20th Century, the horse was replaced by various forms of armored cars or light tanks that could move faster and farther than the formations they supported.[7]

From World War II through Operation Iraqi Freedom, organizational design in cavalry formations fluctuated from light and mobile to heavy and armored. The debate within the cavalry community throughout this period centered on the question of how best to simultaneously equip a cavalry unit with the essential mobility to gain and maintain contact with an enemy force over large distances while preserving the versatility to respond to unexpected threats and fight for information once that contact was achieved.[8] Because of this requirement for versatility, cavalry formations often incorporated combined arms at much lower echelons than other units.

Cavalry in the Cold War-era saw the close integration of attack and reconnaissance helicopters with ground tactical units at squadron level. This design gave the reconnaissance commander the flexibility to collect and fuse intelligence gathered in both the air and land domains into a coherent picture.

In 2017, the U.S. Army published the functional concept for movement and maneuver, which sought to define how it would operate in the period from 2020 to 2040. Derived from the Army’s future operating concept, “multi-domain battle,” this document affirmed the importance of effective and capable reconnaissance operations in the future as one of its foundational principles.[9] It also introduced the concept of “cross-domain maneuver,” which proposed that future U.S. Army forces would “create synergy with capabilities employed across all domains,” including the cyber domain.[10]

Applying this principle of cross-domain maneuver to today’s reconnaissance doctrine suggests that a future reconnaissance formation must possess the capability to engage the enemy with a versatile set of tools that extract vital information from the enemy and the environment in all three relevant domains: land, air and cyber. For the same reason that 20th-Century cavalry units necessarily incorporated air and ground reconnaissance formations at the lowest possible echelon, future cavalry formations will likely find it essential to incorporate the information-collection capacity of ground, air and cyber reconnaissance formations at the lowest possible level of tactical employment.

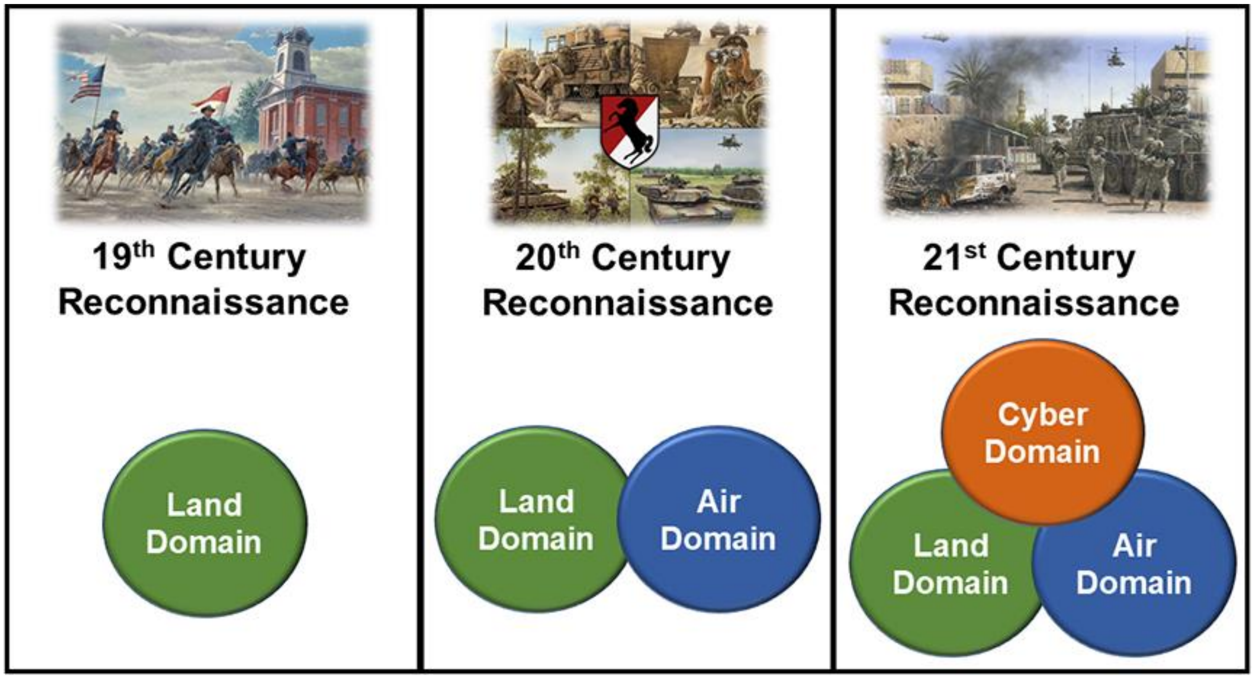
19th Century Reconnaissance
Land Domain
20th Century Reconnaissance
Land Domain
Air Domain
21st Century Reconnaissance
Cyber Domain
Land Domain
Air Domain

Figure 3. As warfare expands into more domains, our concept of reconnaissance operations must expand with it.

Case Study 1: Operation Protective Edge

Before examining how a cyber capability might be designed inside a future cavalry formation, it is useful to examine contemporary conflicts where the exploitation of information from the cyber domain provided a marked tactical advantage to one side.

In July 2014, the kidnapping of three Israeli teenagers, followed by intermittent rocket exchanges between Hamas and Israeli Defense Forces (IDF), led the Israeli government to initiate Operation Protective Edge to reduce or eliminate the rocket threat from the Gaza Strip.[11] The operation lasted 51 days and eventually saw the deaths of thousands of Palestinians and 72 Israeli soldiers and citizens.[12] The campaign was unprecedented in its widespread use of social media and Twitter by both sides to shape the narrative.

The IDF had learned a great deal in their previous incursions into Gaza and understood the value of a capable and responsive social-media presence. For Operation Protective Edge, they stood up a 24-hour social-media response team called the Spokespersons Unit that tailored messages to various media platforms with the IDF perspective on events.[13] To enable their messaging, the unit tracked all relevant social-media feeds emanating from the conflict zone.

A critical test of this cell's capability came July 28, when a flurry of tweets from reporters and bloggers within the Gaza Strip claimed that Israeli aircraft had struck both a hospital and a refugee camp with more than 30 civilian casualties. As the story spread rapidly across social media and into mainstream venues, the Spokespersons Unit tried to get clear answers from IDF commanders, who had no knowledge of the event. Within 80 minutes of the first tweet, the IDF assessed that both strikes had been the result of misfired Hamas rockets. Although 80 minutes was an eternity in the context of modern media, the ability to respond quickly with a clear and convincing counter-narrative avoided a much greater setback for the IDF.[14] The ability to see the social-media activity of the battlefield in real time was critical to this rapid response.

While the battle of competing narratives is an important aspect of cyber activity in modern warfare, there is another important lesson to be drawn from this experience. For that critical 80-minute period, it was the Spokespersons Unit and not the tactical commander on the ground who had the dominant situational understanding. The elaborate network of relationships they had established with digitally-enabled citizens in the conflict zone gave them an improved view of the battlefield.

In traditional cavalry language, they had, in effect, established a virtual reconnaissance screen that provided the IDF with early warning of enemy activity – warning they would never have been able to gain through traditional ground-reconnaissance techniques. The Spokespersons Unit was never intended to be a reconnaissance unit but, for those critical minutes, that was exactly what it became. The information it extracted from cyberspace was only useful when it was merged with an ongoing view of the battlefield from the ground maneuver unit.

Case Study 2: Russia in the Donetsk Region

On July 17, 2014, Malaysian Flight 17 was making its way from Amsterdam to Kuala Lumpur on a route that took it directly over the troubled Donetsk region of eastern Ukraine. As it transited Ukrainian airspace, a Russian SA-11 anti-aircraft system engaged the airliner, killing all 283 passengers on board. The Russian military responded quickly by blaming Ukrainian forces for the shoot-down. Equipped with the world's most sophisticated propaganda machine, they quickly produced documents and evidence showing that a Ukrainian fighter jet and anti-aircraft system were within range of the airliner when it crashed.[15]

Eliot Higgins, a private United Kingdom citizen with no intelligence training and no security clearance, did not buy the Russian version of events. Armed only with an Internet connection and a community of amateur enthusiasts connected by his blogsite Bellingcat, he started to unravel the Russian narrative. Using a single photograph of the SA-11 provided by the Ukrainian military, he and his team were able to painstakingly recreate the precise route the vehicle had taken on the date of the attack by geolocating images drawn from various YouTube videos of the area and open-source satellite imagery.[16] They eventually identified the vehicle as Buk 332 of 53rd Anti-aircraft Rocket Brigade.

Within months, Higgins' team expanded their research to show evidence of the vehicle's movement from its home base in Kursk all the way to the Ukrainian border. When the Joint Investigative Team assembled by the Dutch government published its final report two years later, it relied heavily on the Bellingcat evidence and discredited the Russian government's contradictory narrative.

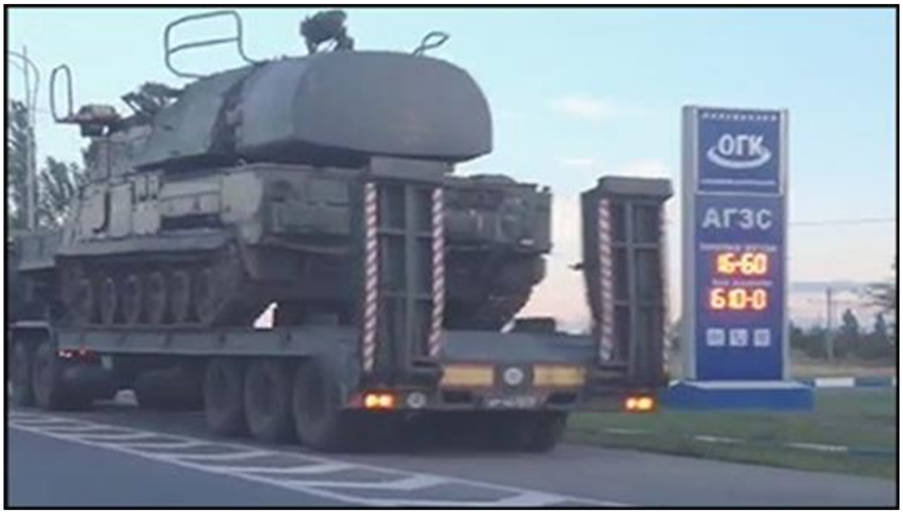

Figure 4. Using this photograph posted on a Russian social-media site, Bellingcat established that Buk 332 had transited Russia prior to shooting down Malaysian Flight 17. *(Photo accessed at https://www.bellingcat.com/news/uk-and-europe/2015/07/16/russias-colin-powell-moment-how-the-russian-governments-mh17-lies-were-exposed)*

This incident, like the one in Gaza, presents a compelling case. Relatively minor tactical actions like the movement of a military vehicle or the firing of a single rocket now leave an indelible fingerprint in cyberspace. That fingerprint is visible to anyone with the persistence, tools and training to view it. This presents a new way of seeing the battlefield. Finding rocket launchers and anti-aircraft weapons on the battlefield in real-time has traditionally been the vocation of reconnaissance formations. Now those reconnaissance organizations must develop new ways of following that information into the cyber domain. Future reconnaissance organizations that are equipped with the ability to merge ground and air collection with this type of capability in cyberspace will possess a competitive advantage on the 21st-Century battlefield.

Crowd-sourced surveillance and future of Internet

Preparing U.S. military forces for the next conflict requires a reasonable forecast of the future operating environment. By 2030, more than 60 percent of the world's 8.3 billion people will live in cities.[17] Rapid urbanization will likely lead to vast slums operating outside of legitimate government control, where political instability and conflict over scarce resources will create a demand for external military intervention. As humanity moves to the city, so too will the warfare it produces.

By 2030, more than 125 billion computers, sensors and appliances will be connected to the Worldwide Web – roughly 15 for every person alive.[18] By that time, nearly 80 percent of the data moving on broadband networks will be video.[19] It is reasonable to assume that these two trends will combine to create a ubiquitous network of crowd-sourced surveillance, where nearly every event in public space is recorded and uploaded to the Web by private, commercial or government actors.

Recent advances in image-recognition technology brought on by machine learning show the potential to transform the utility of this growing mountain of data. Higgins and his team of amateur researchers at Bellingcat were able to geolocate a single vehicle as it transited Russia only after months of painstaking analysis. Image-recognition software may soon compress this process to a matter of hours, if not minutes and seconds.[20] The military formation that can best leverage modern analytical tools to tease out critical information from this vast crowd-sourced surveillance network will have a clear advantage on the dense urban battlefields of the future.

Emerging tools of cyber reconnaissance

History suggests that many of the most significant advances in military technology began first as commercial technologies. Radar, for example, was originally developed as a tool to avoid ship collisions during limited visibility.[21] This section of the article will examine three categories of cyber tools already available in commercial markets that, with adaptation, might provide a real advantage to reconnaissance formations.

Situational understanding through social-media analysis. Humanity today tweets about 6,000 times per second,[22] and this number is expected to rise rapidly over the next 15 years. This storm of data includes commentary and first-person accounts on virtually every event of significance. Modern sentiment-analysis techniques can be applied to this data set to extract opinion trends specific to both topic and location.[23] This technology is increasingly being adapted for its utility in conflict zones where official government accounts are often incomplete and misleading.

For example, Ushahidi, a crowd-sourced application that promotes "social activism for marginalized voices," was created in the violent aftermath of the disputed presidential election in Kenya.[24] Actors in the conflict could submit eyewitness accounts, which were then plotted on a map to show overall trends as violence spread. As just one example, Ushahidi's Syria-Tracker currently provides very detailed, location-specific information that could provide vital insights to a ground-maneuver commander.[25]

Military activity by its very nature is dramatic and tends to draw the interest of onlookers. Whether it is the citizens of Washington flocking to Bull Run with their picnic baskets to observe the first battle of the American Civil War[26] or curious Russians uploading video of a convoy of anti-aircraft weapons on their way to Ukraine, military activity captures human interest and attention. Today and in the future, that interest will almost certainly manifest itself as real-time intelligence across social-media platforms. Intervening amid an internal conflict or outright civil war presents a daunting challenge to an outsider. Tapping into this enormously valuable information stream has the potential to provide superior situational awareness to the commander who can adequately harness it.

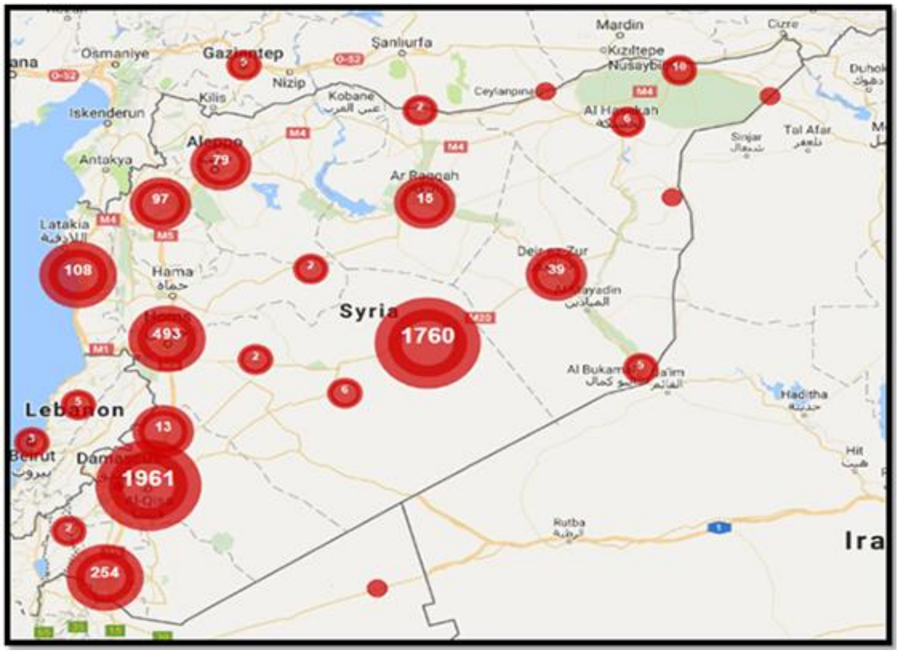

Figure 5. Ushahidi's Syria tracker provides real-world situational awareness of battlefield activity based entirely on social-media posts. *(See https://www.ushahidi.com/case-studies/syria-tracker, accessed May 27, 2018)*

Route reconnaissance using Global Positioning System-enabled device-pattern analysis. The fitness data company Strava recently came under fire when it was discovered that its global heatmap, which aggregated millions of geotracked devices, inadvertently revealed the location and outline of U.S. military bases in conflict areas.[27] While this incident provides a useful reminder about the importance of operational security, it reveals a much more valuable message about the future of route reconnaissance as a military operation.

Moving a large military force over unfamiliar terrain presents a formidable challenge. As a result, reconnaissance formations have traditionally needed to reconnoiter ahead of the main body to assess the trafficability of routes. Like Strava, modern digital-map applications on most smartphones use a process of extracting location from celltowers to determine rates of movement along roadways.[28] Over time, this anonymized data provides a useful pattern that can show where vehicle traffic is unrestricted, moderately restricted or impassable. It can, therefore, be a powerful tool to augment the often-dangerous task of ground route reconnaissance. In addition, when merged with Ground Moving Target Indicator data from aerial reconnaissance platforms, this data can also provide a useful analytical tool to distinguish between civilian and military vehicle movement.

Near-real-time commercial-satellite imagery. The rapid growth of commercially available satellite imagery has had a profound effect on the utility of aerial surveillance. Today, Digital Globe, the world's largest public repository of satellite imagery, estimates that it retains a dataset of 100,000 terabytes (Tb) of data that grows daily by 100 Tb.[29] Digital Globe's recent deployment of constellations of tiny commercial CubeSats will further expand this data-collection capacity by dramatically reducing refresh times for new imagery down from a matter of days to a matter of hours.[30] With this emerging capability, it is entirely reasonable in the near future to expect commercial users to obtain sub-meter-resolution satellite imagery less than 24 hours after image capture.

The timeliness of this information flow moves spaced-based intelligence collection from the strategic and operational level to the tactical level. It would make little sense to send military formations into a dangerous area without the benefit of current high-resolution imagery that is less than 24 hours old and freely available to commercial users with a subscription to Digital Globe or a similar dataset.

Perils of cyber reconnaissance

The expansion of reconnaissance into the cyber domain presents some unsettling challenges to our familiar concept of warfare as a purely public and professional activity separate and distinct from our personal lives.

Because of its ability to transcend geography, the cyber domain blurs the distinction between public and private life. For example, the Bellingcat investigation discussed earlier led to a blogsite where mothers of Soldiers in 53rd Anti-aircraft Rocket Brigade shared pictures of their sons.[31] If a U.S. cyber scout had arrived at this site, would it be lawful to extract military intelligence from a mother's social-media post? Would it be ethical not to if that intelligence could protect friendly forces from harm? Likewise, is it ethical to use a crowd-sourced Website like Ushahidi that seeks to give a voice to victims of political violence as a tool of military reconnaissance?

Considering how a future adversary might employ the tools outlined above to conduct his own version of cyber reconnaissance presents an even more daunting challenge. In 2014, the Islamic State in Iraq and Syria (ISIS) published a "kill list" with the home addresses of 100 U.S. servicemembers that it believed were associated with the air campaign in Iraq and Syria.[32] While no hostile action resulted from the kill list, it presents a significant challenge to the very idea of military service in a free and open society. The emergence of reliable face-matching technology will only make it more difficult to separate personal and professional identities. The military utility of the cyber domain presents some fundamental questions about the proper boundaries of military activity in that space, and these will require careful examination and clear policy guidelines as this capability is fully exploited.

A second peril of using the cyber reconnaissance to inform battlefield decision is that, like other forms of intelligence, it can simply be wrong. Big data does not necessarily mean good data. The recent experience of Google Flu provides a useful example. In 2008, Google began predicting the progress of flu outbreaks across the United States by tracking flu-related search terms on its Website. Initially, the data appeared to provide more rapid indicators of flu outbreaks than the standard methods of hospital reporting used by the Centers for Disease Control. This rapid-response time, however, came at a price in terms of the accuracy of reporting and sensitivity to false positives. Ultimately, Google scrapped the project because of its potential to produce very specific, highly-credible but entirely inaccurate information.[33]

There is a real risk of cyber-reconnaissance efforts providing equally compelling yet misleading false positives, especially in the face of a concerted effort to confuse or distract that reconnaissance with the employment of Twitter bots or other tools that create a false footprint of activity in the cyber domain. Intelligence gathered from the cyber domain is no different from intelligence extracted from more traditional domains. It should be carefully vetted against other sources of information gathered from complementary methods of reconnaissance.

Isn't this someone else's job?

It might be tempting to dismiss cyber reconnaissance as unsoldierly work that should be carried out by some department of "other people" far from the battlefield. The problem with this approach is that reconnaissance information is only useful when it is narrowly focused on a commander's specific and immediate needs, and when it is fused with information gained from other sources. Both conditions emerge at the tactical edge, where the rapidly changing dynamics of the battlefield create a constant stream of new information requirements and where fleeting opportunities are seized and exploited. Cavalry formations directly support maneuver commanders and have operated in this chaotic space since their inception. As a result, they are uniquely qualified to provide the most responsive support to the maneuver commander.

The cyber scout is not in the business of producing military effects in the cyber domain and therefore does not need the extensive authorities of a more traditional cyber warrior. While he may "fight for information" in cyberspace in some very limited circumstances, his primary task is to master the tools of open-source information collection and to harness those tools in pursuit of his commander's priority information requirements. He does not need to be an experienced hacker, but he does need to understand the very specific information requirements of the maneuver commander he supports. The two lieutenants in 1/4 BCT's cyber-recon team succeeded not because they were experts on social media but because they understood the fundamentals of good reconnaissance and could apply those creatively in a different domain. Likewise, the cyber scout must be "born" a scout first and then taught to apply his trade in a new domain.

It may seem farfetched today to envision a future cyber-recon platoon sitting at a bank of Internet terminals, surfing Twitter and YouTube feeds to assist a cavalry troop on a screen line. But it does not require an excess of imagination to see its obvious utility, particularly in a world that has 15 Internet-enabled devices for every human alive. Cavalry organizations have traditionally succeeded when they were designed with inherent versatility by combining all the various means of information collection into agile organic small-unit formations. We cannot succeed by relegating this tactical information-collection activity to some department that is organizationally and geographically separated from the customer it supports. Expanding the role of cavalry into the cyber domain will require the same commitment to combined-arms capability that made our 20th-Century cavalry squadrons so effective.

Conclusions

Professional armies have a long-established track record of fighting today's wars with yesterday's thinking. History demonstrates that the bureaucratic and institutional pressures to favor well-established experience in the face of technological change are nearly insurmountable, absent some compelling urgency to act. For example, the concept of aerial reconnaissance was first born in 1794 when the world's first surveillance balloon lifted above the battle of Fleurus in France. More than a century would pass before professional armies would invest enough energy to overcome the technical challenges associated with using aerial reconnaissance effectively. Once they mastered it, more than a century later in World War I, it had a profound effect on the character of conflict.

The only thing harder than getting new ideas in is getting the old ones out. A cursory review of ***Cavalry Journal***s in the 1930s will provide a modern cavalryman with a surreal experience. Well-respected and thoughtful leaders as late as 1939 argued repeatedly that proper reconnaissance, even in the mechanized battles to come in Europe, could only happen on horseback.[34] The horse had been the primary tool of the scout for centuries, and most could not imagine battlefield reconnaissance occurring without it. Unfortunately, history reminds us often that nostalgia is a poor force-design principle.

Experienced cavalry leaders today may argue that effective reconnaissance cannot be done from the sanctuary of a computer screen. In this they are partially correct. Nothing will replace the scout on the ground in visual contact with the enemy. But to send that scout into harm's way to collect information freely available in some unexplored corner of the Internet is a travesty. Battlefield information is migrating into the cyber domain, and the scouts who hunt for that information must follow it there. What we need is the ability to effectively fuse complementary sources of information from the ground, air and cyber domains to paint a coherent picture for our battlefield decision-makers.

When the United States and its allies invaded Iraq in 2003, Facebook and Twitter did not exist, and the smartphone was nothing more than a design concept. Since that time, these tools of individual empowerment have diffused traditional sources of power to topple governments and transform societies. In 2003, surveillance was the business of government. Since that time, the emergence of a ubiquitous, crowd-sourced surveillance network composed of billions of Internet-enabled devices marks one of the most profound shifts in our society today. These changes have fundamentally altered the boundaries between public and private life and between war and peace. As recent conflicts have already shown, this transformation will alter the way wars are fought in the future. If reconnaissance is about the business of fighting for information, then the U.S. Army must rethink and reframe its approach to reconnaissance in the Information Age.

COL Curt Taylor is chief of staff, 1st Infantry Division, Fort Riley, KS, and an active-duty cavalry officer. (He emphasizes that this article does not reflect official 1st Infantry Division policy.) Previous assignments include commander, 1st Stryker Infantry Brigade, 4th Infantry Division, Fort Carson, CO, reorganizing it to train and fight as the Army's first reconnaissance-and-security BCT; commander, 3-66 Armor, 172nd Infantry Brigade, Paktika, Afghanistan, and Grafenwoehr, Germany; and commander, Troop A, 4-7 Cavalry, Camp GarryOwen, Korea. His military education includes Higher Command and Staff College, Shrivenham, United Kingdom; Army Strategic Leadership Study Program at Fort Leavenworth, KS; Command and General Staff College (CGSC); Armor Captain's Career Course; and Armor Officer Basic Course. COL Taylor holds two master's of military arts and science degrees: in strategic studies from the School of Advanced Military Studies and in military art and science from CGSC.

Notes

[1] Maksymillian Czuperski et al., "Hiding in Plain Sight: Putin's War in Ukraine," ***Atlantic Council***, 16, accessed Feb. 18, 2018, http://www.atlanticcouncil.org/publications/reports/hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov-s-putin-war.

[2] Lahav Harkov, "Gaza Reporters' Tweets: Hamas Using Human Shields," ***Jerusalem Post***, July 24, 2014, accessed Feb. 18, 2018, http://www.jpost.com/Operation-Protective-Edge/Gaza-reporters-tweets-Hamas-using-human-shields-368689.

[3] LT Christopher Lowman and LT Gerald Prater, whitepaper "Expansion of the Reconnaissance and Security BCT into the Cyber Domain: Lessons Learned from NTC Rotation 17-07.05," published July 17, 2017. The cyber-recon team in 1/4th Infantry Division was an experimental element of the reconnaissance-and-security BCT excursion. Geolocation of OPFOR augmentee units was generated by a Snapchat heatmap application and by triangulating distances from multiple locations using the dating site Tinder's range estimator. Of note, superb digital OPSEC in 11th Armored Cavalry Regiment severely inhibited cyber exploitation of permanent-party OPFOR. Augmentee OPFOR, however, were easily detected and located using conventional social media.

[4] Elizabeth Harman Pakenham Longford, ***Wellington: The Years of the Sword***, New York: Harper, 1972.

[5] Department of the Army, U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-6, ***U.S. Army Functional Concept for Movement and Maneuver***, Washington, DC, 2017.

[6] Department of the Army, Field Manual 3-98, ***Reconnaissance and Security Operations***, Washington, DC, 2017.

[7] Robert S. Cameron, ***To Fight Or Not To Fight?: Organizational And Doctrinal Trends In Mounted Maneuver Reconnaissance From The Interwar Years To Operation Iraqi Freedom***, Fort Leavenworth, KS: Combat Studies Institute Press, U.S. Army Combined Arms Center, 2010.

[8] Ibid.

[9] TRADOC Pamphlet 525-3-6.

[10] Ibid.

[11] Raphael S. Cohen et al, ***From Cast Lead to Protective Edge: Lessons from Israel's Wars in Gaza***, Santa Monica, CA: RAND Corporation, 2017.

[12] Ibid.

[13] David Patrikarakos, ***War in 140 Characters: How Social Media is Reshaping Conflict in the Twenty-First Century***, New York: Basic Books, 2017, Kindle version.

[14] Ibid.

[15] Eliot Higgins, "How the Russian Government's MH17 Lies Were Exposed," Bellingcat, Sept. 26, 2016, accessed Feb. 22, 2018, https://www.bellingcat.com/news/uk-and-europe/2015/07/16/russias-colin-powell-moment-how-the-russian-governments-mh17-lies-were-exposed.

[16] Patrikarakos.

[17] U.S. National Intelligence Council, ***Global Trends 2030: Alternative Worlds***, Washington, DC: Government Printing Office, 2012.

[18] Jenalea Howell, "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says," IHS Markit Technology, Oct. 24, 2017, accessed Feb. 22, 2018, https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says.

[19] Sophie Curtis, "5G Future: Experts Predict the Future of Mobile Networks," ***The Telegraph***, May 17, 2014, accessed Feb. 22, 2018, http://www.telegraph.co.uk/technology/mobile-phones/10837056/5G-future-experts-predict-the-future-of-mobile-networks.html.

[20] Jerry Kaplan, ***Artificial Intelligence***, Oxford: Oxford University Press, 2016.

[21] Robert Buderi, ***The Invention That Changed the World: How a Small Group of Radar Pioneers Won The Second World War and Launched a Technical Revolution***, New York: Touchstone, 1997.

[22] "Behind the numbers: tweets per minute," Twitter, accessed Feb. 19, 2018, https://blog.twitter.com/official/en_us/a/2013/behind-the-numbers-tweets-per-minute.html.

[23] Alexander Pak and Patrick Paroubek, ***Twitter as a Corpus for Sentiment Analysis and Opinion Mining***, report, proceedings of LREC, 2010.

[24] Ory Okolloh, "Ushahid or 'Testimony': Web 2.0 Tools for Crowdsourcing Crisis Information," ***Change at Hand: Web 2.0 for Development***, IIED and CTA, 2009.

[25] See https://www.ushahidi.com/case-studies/syria-tracker, accessed May 27, 2018.

[26] Eugene C. Tidball**, *No Disgrace to my Country: the Life of John C. Tidball***, Kent, Ohio: Kent State University Press, 2002.

[27] Liz Sly, "U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging," ***The Washington Post***, Jan. 29, 2018, accessed Feb. 19, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.80a2ff483b78.

[28] Raffi Sevlian, ***Travel Time Estimation Using Floating Car Data,*** thesis, Stanford University, 2010.

[29] Sarah Scoles, "The Best Way to Transmit Satellite Data? In Trucks. Really," ***Wired Magazine***, May 17, 2017, accessed Feb. 19, 2018, https://www.wired.com/2017/05/best-way-transmit-satellite-data-trucks-really/.

[30] Keith Cowing, "28 Cubesats Launched from the Space Station," ***SpaceRef***, Feb. 11, 2014, accessed Feb. 22, 2018, http://spaceref.com/nasa-hack-space/28-cubesats-launched-from-the-space-station.html.

[31] Patrikarakos.

[32] Tom Wilson, "ISIS releases hit list of 100 American military personnel," ***New York Post***, March 22, 2015, accessed Feb. 19, 2018, https://nypost.com/2015/03/22/isis-releases-hit-list-of-100-american-military-personnel/.

[33] David Lazer and Ryan Kennedy, "What We Can Learn from the Epic Failure of Google Flu Trends," ***Wired Magazine***, Oct. 1, 2015, accessed Feb. 19, 2018, https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/.

[34] ***Cavalry Journal***, Volume XLVIII, 1939, contains many examples of impassioned defense of the horse as an effective scout platform on the mechanized battlefield in Europe. Most notably see "May I Say a Word for the Horse," accessed May 25, 2018, http://www.benning.army.mil/library/content/Virtual/CavalryArmorJournal/1930s /1939Jan-Jun.pdf.

Acronym Quick-Scan

BCT – brigade combat team
CGSC – Command and General Staff College
IDF – Israeli Defense Forces
ISIS – Islamic State in Iraq and Syria
NTC – National Training Center
OPFOR – opposing force
TB – terabyte
TRADOC – (U.S. Army) Training and Doctrine Command