The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation

Dr. Dan G. Cox

ABSTRACT

Battle space is increasingly transparent. This transparency includes not only electronic signatures but also other actors in the environment. Cell phones today make the movement of military troops and equipment particularly problematic. In order to safely maneuver on the future battlefield, this article proposes the development of a cyber smoke screen. Unfortunately, such a smoke screen, while defensive in nature, would require temporary disruption of local internet and cellular access, thereby bringing this essential defensive maneuver under offensive cyber operations, which implicates both strategic and moral concerns.

INTRODUCTION

As the U.S. military refines its concept for All-Domain Operations (ADO),[1] many new military necessities and problems arise. Preparing for these challenges in advance of prosecuting a war will lead to greater success. This article focuses on a future cyber smoke screen as a pressing example of the complexity of ADO and provides three cogent examples as to why this has become a battlefield imperative. This will be followed by a discussion of related moral and strategic considerations. Finally, the use of a cyber smoke screen is offered to the reader.

WHY A CYBER SMOKE SCREEN IS NEEDED ON THE MODERN BATTLEFIELD

Examining what enemies struggle with on the battlefield is one cogent way to adapt to the future of warfare. The Islamic State in Iraq and Syria (ISIS), the Russian military, and

Dr. Cox has worked with the U.S. Department of Defense and the U.S. Army for seventeen years, including work with U.S. Army Futures Command, the NATO Partnership for Peace Program, improving the professional military education system for the Republic of Armenia's military, and teaching elite military planners operational art and design at the School of Advanced Military Studies (SAMS). He has three published books: *Terrorism, Instability and Democracy in Asia and Africa, Population-Centric Counterinsurgency: A False Idol, and Stability Economics: The Economic Foundations of Security in Post-Conflict Environments*. Dr. Cox is currently researching future warfare, especially issues of cybersecurity, disinformation, the future of design and military planning, and fictional scenarios.

the Ukrainian military have recently demonstrated that cyberspace can be weaponized. And ISIS attempting to stop the weaponization of cyberspace against them failed. Russia too has failed to prevent the weaponization of cyberspace by Ukraine. Still, they seem to have adapted in a way that has prevented further exploitation. As the battlefield becomes more transparent, the need for new ways to hide becomes increasingly important, as illustrated in more detail below.

While ISIS consolidated territorial gains in the Middle East, key leaders became concerned about citizens in controlled areas having access to the internet. ISIS was concerned about online sources leaking information counter to their extreme religious teachings. In the Fall of 2014, ISIS banned all internet access in the key Iraqi city of Mosul.[2] This total ban of the internet in Mosul had disastrous consequences for the local populace. Many local businesses were unable to operate, some services went offline, and residents felt disconnected from the world and their families abroad.[3] ISIS refined its approach in Raqqa, Syria. Instead of banning internet access, ISIS banned private providers but increased the number of ISIS-controlled internet cafes, and even required its own soldiers to use the ISIS-controlled cafes.[4]

As time went on, ISIS continued to control internet access, but they did not again engage in unpopular internet blackouts. Once ISIS realized that the real tactical and operational problem came from cell phones, it began focusing on them. Cell phones not only gave Iraqi and Syrian citizens access to counternarratives, they also could turn these same citizens into sensors, thereby facilitating western forces that were targeting them.[5] While ISIS was able to control broadband, 3G allowed citizens to access the internet and post pictures instantly, which led ISIS again to opt for a total ban on internet access for cell phones.[6] ISIS commandeered all SIM cards, allowing citizens to

take pictures but preventing any sending of text or visual information. Citizens reported feeling as if they had "gone back to the stone age."[7]

Russia's experience with cell phones is more recent and more painful. The most current Russian casualty count with Ukraine is 615,000, with an estimated 115,000 of those forces killed in action.[8] The Russian military is now admitting that many troops were successfully targeted through cell phones.[9] Some of this targeting came through a lack of cell phone discipline. For example, unauthorized use of cell phones by Russian soldiers is the transparent battlefield John Antal warns about, which allowed Ukraine to target a temporarily base of Russian soldiers in Ukraine, resulting in 89 Russian soldiers being killed.[10] More recently, analysts have noted that Russia and Ukraine use cell phone signatures and information aggregators.[11] Antal is correct. The battlefield is becoming more transparent than ever. The idea that masking, the ability to hide maneuvers and formations, is of prime importance.[12]

Open-source aggregation sites further increase battlefield transparency. The website Live Universal Awareness Map (liveuamap.com) began posting conflict information in 2014, and relies on social media, often from freelance reporters and citizens on the ground during conflicts, using embedded geotags to verify the location of social media posts and pictures. "The data is collected by 'AI web crawlers,' which filter relevant stories that are forwarded to a group of expert analysts for fact-checking,"[13] and covers many conflicts, e.g., Ukraine, Gaza, the war in Syria, the war in Afghanistan, ISIS, Al-Qaeda, and Al Shabab.[14] U.S. Marine Corps Lieutenant General (Lt. Gen.) Karsten Heckl noted a growing "ubiquity and proliferation of sensors" on the battlefield.[15] Lt. Gen. Heckl notes that battlefield sensors increasingly allow for a quick and effective targeted kill.[16] Both Russia and Ukraine have suffered losses from the latest mobile, intelligence-driven sensors: humans with cell phones. AI-driven aggregators of social media posts will only exacerbate this danger to maneuvering forces.

A more recent incident brings the need for a cyber smoke screen into sharp focus. On September 17 and 18, 2024, Israel conducted stunning attacks against Hezbollah leadership and operatives.[17] The attacks resulted in dozens of Hezbollah operatives killed and thousands more wounded.[18] Hezbollah had recently ordered new pagers and walkie-talkies as to which Israel had infiltrated the production chain, embedding small explosive charges into each device.[19] These attacks make cell phone-enabled Improvised Explosive Device (IED) attacks in Iraq and Afghanistan against U.S. soldiers look archaic by comparison. One can imagine a future battlefield where multiple cell phone-enabled explosives line logistical routes making the need for a cyber smoke screen even greater.

Hiding, camouflage, and other masking techniques remain critically important. Future battlefields likely will become increasingly more dispersed than battlefields of the past. Still, large and small formations will have to traverse the transparent battlefield, and militaries will be able, when opportune, to mass or converge on opposing units. Logistical supply must also traverse dangerous battlefields. All the operational movements on the battlefield will

require the ability to thwart as many sensors as possible and one of the most effective sensors on today's battlefield is the cell phone-armed person on the ground, thereby enhancing the need for a cyber smoke screen, the implementation of which is discussed below. Simply put, an effective cyber smoke screen will serve to temporarily arrest internet functionality and cellular services for just long enough to allow military units safe maneuver without detection.

THRESHOLD CHALLENGES IN IMPLEMENTING A CYBER SMOKE SCREEN

The need for cyber smoke screens is clear and, as discussed below, implementing this raises ethical and other strategic challenges. The final section of this article proposes ways to employ cyber smoke screens that address and accommodate some of these challenges.

When ISIS shut down internet access for the people of Mosul for an extended period, it likely violated International Humanitarian Law (IHL). No specific IHL governs cyberspace, but corollary IHL rules do govern the denial of water or food. IHL governing *jus in bello*, or the just prosecution of war, provides a framework for boundaries that should guide militaries in modern warfare.

Capturing both the IHL inherent in the Geneva Accords and expanding the notions to modern war, Michael Walzer's book, *Just and Unjust Wars*,[20] provides a good starting point for this discussion. Walzer's concept of proportionality and double effect are particularly apt here. Walzer lays out the principle of double effect as a common occurrence in war whereby normal and necessary military operations often put non-combatants at risk or in harm's way. The military action has the double effect of being a good, legitimate, and military necessary action in war, yet unintentionally harmful to innocent civilians.[21] Walzer lists four criteria for a just action in a war that poses a high risk of double effect. Of these, the fourth criterion, "proportionality," is particularly pertinent to this discussion. Walzer argues, "the good effect [must be] sufficiently good to compensate for allowing the evil effect."[22] In other words, the harm befalling civilians must be less than the military benefit or necessity.

The Geneva Conventions echo the concepts of "proportionality" and "military necessity." Article 3 requires that non-combatants, including prisoners of war, be treated as humanely as possible.[23] Article 53 deals explicitly with military necessity, and prohibits destroying civilian property unless compelling and necessary for military operations.[24] These two prohibitions on harm to civilians and civilian property nest nicely with aspects of civilian life that should never be intentionally disrupted, regardless of military need, such as water or food. IHL renders the disruption of water supplies to civilians an explicit war crime.[25] IHL on cyberspace remains to be developed, but clearly, while the internet is vital to a modern functioning society, it is nowhere near as pressing as the human need for water and food. Still, caution and mindfulness are essential when military necessity requires large-scale and prolonged disruption of internet services.

Reviewing the ISIS ban on the internet is instructive here. The ban was instituted for two reasons. First, ISIS did not want foreign ideas to infiltrate their caliphate. Second, ISIS leaders worried that geo-location tags on pictures from cell phones and other social media posts would help Iraqi and Western military operators target key leadership more effectively.

The first reason for internet disruption hardly fits the definition of military necessity, but the second reason – avoiding targeting bulls-eyes – clearly fits. However, enforcing that ban by ISIS was both disproportional and also a war crime. When ISIS detained and burned alive citizens in Mosul caught with a cell phone sim card,[26] the military necessity rationale was clearly overwhelmed by the proportionality guard rails of IHL.

Further, a blanket denial of internet access for months or years caused such significant economic and psychological damage to the citizens of Mosul that it would violate Walzer's notion of double effects in war if the harm to civilians outweighed the military benefit of the operation. Even in terms of effectiveness, disruption of internet services in Mosul seems counterproductive. From a simple counterinsurgency standpoint, cutting off civilians from the internet for a prolonged period undoubtedly cause deep resentment against the occupying forces. Minimizing that resentment is a factor the U.S. should keep in mind in future military operations.

Beyond these moral considerations, cyber smoke screens pose other strategic complexities, such as the way U.S. Cyber Command (USCYBERCOM) is organized with offensive and defensive cyber operations (OCO/DCO) separated as siloed and distinct entities creates further problems.[27] So far there is much less analysis of OCO in the literature, and most U.S. cyber operations remain defensive in nature.[28] USCYBERCOM expanded its notion of cyber operations in 2018, but this all was mainly aimed at expanding defensive operations. In 2018, the notion of defending forward came into vogue. Instead of simply defending the homeland, USCYBERCOM would now partner and help allies defend from cyberattacks from adversaries, ensuring that forces and capabilities of allied nations' military and infrastructure assets and U.S. military assets abroad remained safeguarded.[29]

Even in a predominantly defensive role, USCYBERCOM realizes that the innate interconnected nature of cyberspace means that the U.S. will be in constant contact with adversaries and enemies. Therefore, defending forward is married with the notion of persistent engagement in cyberspace. However, this persistent nature is almost exclusively defensive in nature. An Offensive Cyber Operation (OCO) will mainly occur either to prevent an attack or during a war. Even during a war, OCO authorities still largely reside at the Strategic level, mainly with the U.S. president.[30]

There are compelling reasons why OCO is so hard to enact. The authorities for OCO are held at the highest level in the United States. As Austin Long notes, it takes guidance from the National Command Authority (NCA) to develop potential strategic OCO, and no known directives or authorities exist at the operational or tactical level.[31]

What is ironic about this current article is that what seems to be, on the surface, a defensive cyber operation, a cyber smoke screen, is also immediately offensive. Military operators will have to disrupt local internet networks to establish the cyber smoke screen and effectively mask military maneuvers. ISIS, Russia, and Ukraine have all been negatively affected by using cell phones on the ground. The advent of aggregator websites like Liveuamap makes the need for masking movement from people with cell phones even more pressing.

CYBER SMOKE SCREENS FOR FUTURE WAR

The need for masking military maneuvers is only going to grow over time. Assuming authorities for at least limited OCO will be pushed down to the operational and tactical levels, what should a moral and operationally sound cyber smoke screen look like?

As to moral implications, some international legal scholars likely will argue that internet access is like water and, hence off limits even in war. But the internet arguably is not a basic need. While integral to modern economic activity, it can be disrupted. The debate more properly should be focused on duration, and not the consequences of an indefinite disruption of internet services. The military necessity of a cyber smoke screen is compelling. Military maneuvers are too risky to conduct with millions of sensors on the ground constantly compromising positions via civilian cell phones. This does not mean it is militarily prudent or morally correct to follow the spirit of IHL to disrupt internet and cell phone services broadly for a prolonged period.

Instead, a cyber smoke screen would comprise a temporary disruption of the internet and cell phone services (several hours at most) to allow military units to maneuver through the terrain, especially urban areas, without showing up on aggregation websites and targeting schemes of enemy forces.

A single cyber smoke screen along one route will be insufficient since the outage trajectory itself might give the enemy a good idea of where forces are headed. Therefore, two or more cyber smoke screens may need to be deployed simultaneously to deceive and present a dilemma to enemy forces and prevent or at least greatly diminish the opportunity to mass on U.S. forces. Each cyber smoke screen would take a distinct and significantly different route through the terrain. Two would be fakes and one would mask the real military movement. This tactic would increase the chance of successfully moving through an area undetected while reducing the risk of movement. Human intelligence could easily thwart this system, but cell phones would be mitigated as a means of exposure.

This means that USCYBERCOM must accelerate its mixing of offensive and defensive cyber operations. The notion of a cyber smoke screen also illustrates the dual and simultaneous nature of many necessary tactical and operational cyber operations. This means that USCYBERCOM must be given more authorities for OCO, which it has to push down to the operational

and tactical level. Further, USCYBERCOM must reintegrate OCO and DCO operations and units as they recognize that cyberspace does not easily fit into separate silos of offense and defense. Failure to adapt means U.S. troops will be exposed to the risk of being placed in a quick-kill chain by the enemy.

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the School of Advanced Military Studies, the Department of the Army. or the Department of Defense.

NOTES

1. It should be noted that joint publications refer to ADO, but U.S. Army doctrine refers to Multi-Domain Operations (MDO) which means basically the same thing. Department of the Army. *FM 3.0 Operations*, (October 2022).
2. Associated Press, "ISIS Blocks Mobile Phone Networks in Largest City They Control," (November 27, 2014). AP Report on *CBS News Online*, https://www.cbc.news.com/news/isis-blocks-mobile-phone-networks-in-mosul./.
3. Associated Press, "ISIS Blocks Mobile Phone Networks in Largest City They Control."
4. Al Jazeera, "ISIL Bans Private Internet Access in Syria's Raqqa," (July 20, 2015). *Al Jazeera News Online*, https://www.aljazeera.com/news/2015/7/20/isil-bans-private-internet-access-in-syrias-raqqa.
5. Benjamin Plackett, "Burned Alive for Using a Smartphone," (Updated April 5, 2019). *Engadget Online,* (https://www.engadget.com/2019-04-05-isis-mosul-occupation-killed-for-smartphone.html.
6. Benjamin Plackett, "Burned Alive for Using a Smartphone."
7. Benjamin Plackett, "Burned Alive for Using a Smartphone."
8. Eric Schmitt, "September Was Deadly Month for Russian Troops in Ukraine, U.S. Says," (October 10, 2024). *The New York Times*, https://www.nytimes.com/2024/10/10/us/politics/russia-casualties-ukraine-war.html.
9. Helene Cooper, Thomas Gibbons-Neff, Eric Schmitt, and Julian E. Barnes, "Troop Deaths and Injuries in Ukraine War Near 500,000, U.S. Officials Say," (August 18, 2023). *The New York Times*, https://www.nytimes.com/2023/08/18/us/politics/ukraine-russia-war-casualties.html.
10. Colonel (Retired) John Antal, *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting.* (February 3, 2022). New York: Casemate, 4; and Felipe Dana, "Russia Says Phone Use Allowed Ukraine to Target Its Troops," (January 4, 2023). *Associated Press,* https://www.military.com/daily-news/2023/01/04/russia-says-phone-use-allowed-ukraine-target-its-troops.html.
11. Chris Stokel-Walker, "Russia and Ukraine are Both Weaponising Mobile Phones to Track Troops," (April 11, 2022). *New Scientist*, https://www.newscientist.com/article2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/.
12. John Antal, *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting*, 143.
13. *European Union Data Portal,* "Live Universal Awareness Displays Events Related to Russia's Invasion of Ukraine." (May 27, 2022). https://data.europa.eu/en/news-events/news/live-universal-awareness-map-displays-events-related-russias-invasion-ukraine.
14. Liveuamap, LLC, *Live Universal Awareness Map*, (June 9, 2024). API operated from McLean, Virginia using European Union Infrastructure, https://liveuamap.com.
15. John M. Doyle, "General: Precise Sensors to Close Kill Chain Is a Key Takeaway from Ukraine," (May 5, 2022). *Seapower Magazine*, https://seapower.magazine.org/general-precise-sensors-to-close-kill-chain-is-a-key-takeaway-from-Ukraine.
16. John M. Doyle, "General: Precise Sensors to Close Kill Chain Is a Key Takeaway from Ukraine."
17. Kat Lonsdorf and Itay Stern, "From pager blasts to Nasrallah's killing: 12 days that transformed a bloody conflict." (September 29, 2024). *NPR*. (accessed Oct 5, 2024). https://www.npr.org/2024/09/29/g-s1-25348/israel-hezbollah-lebanon-hassan-nasrallah-timeline.
18. Matt Murphy, "What We Know About the Hezbollah Device Explosions," (September 20, 2024). BBC News. (Accessed October 5, 2024). https://www.bbc.com/news/articles/cz04m9l3m49o.
19. Jonathan Yerushalmy and Dan Milmo, "Hezbollah device blasts: how did pagers and walkie-talkies explode and what do we know about the attacks?" (September 18, 2024). *The Guardian*. (accessed October 5, 2024). https://www.theguardian.com/world/2024/sep/18/hezbollah-pagers-what-do-we-know-about-how-the-attack-happened.
20. Michael Waltzer, Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, (1977). New York: NY: Perseus Books Group: 152-53.
21. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 152-153.
22. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 152-153.
23. *Geneva Convention Relative to the Protection of Civilians in Time of War. 12 August 1949. Article 3, Conflicts Not of an International Character,* (June 7, 2024). Geneva: International Committee of the Red Cross, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-3.

NOTES

24. *Geneva Convention Relative to the Protection of Civilians in Time of War. 12 August 1949. Article 53, Prohibited Destruction*, (June 7, 2024). Geneva: International Committee of the Red Cross, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-53.
25. Peter H. Gleick, "It's Vital to Protect Water Infrastructure During War," (June 7, 2023). *Time*. https://time.com/6285314/ukraine-dam-destruction-water-war-essay/.
26. Benjamin Plackett, "Burned Alive for Using a Smartphone."
27. U.S. Cyber Command Public Affairs, "Cyber 101 – Cyber Mission Force," (November 1, 2022). https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission.
28. Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." (February 18, 2017). *Journal of Cybersecurity*. Issue 3, No. 1, https://academic.oup.com/cybersecurity/article/3/1/19/3003367, 19.
29. Nina Colliers and Jacquelyn Schneider. "Defending Forward: The 2018 Cyber Strategy is Here," (September 20, 2018). *War on the Rocks*, https://waronthrocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.
30. Michael P. Fisherkeller and Richard J Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," (December 9, 2019). *The Cyber Defense Review, Special Edition, International Conference on Cyber Conflict* (CYCON U.S.), 269-70.
31. Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," 20.