Mad Scientist Laboratory Blog Post 405 (30 June 22)

405. Democratized Intelligence

[**Editor's Note:** Army Mad Scientist welcomes back guest blogger **Kate Kilgore** with another insightful signpost to the future from the on-going conflict in Ukraine — Democratized Intelligence. Until recently, the ability to Process, Exploit, and Disseminate (PED) meaningful intelligence in a timely manner to directly influence combat operations was the purview of only a finite number of nations with access to Low Earth Orbit providing the requisite imagery and direct link communications capabilities.

No more! Within the past decade or so, access to the **Space domain** has been democratized, with the advent of a host of commercial enterprises (e.g., ***SpaceX***) willing to boost payloads into LEO. And with this capability, other commercial entities (e.g., ***MAXAR***) now provide high resolution imagery services of virtually the entire Earth's surface (down to 30 cm!) with great accuracy (90% confidence that the identified feature is within a 4 meter radius of where the image suggests it is!) on demand. With the emergence of **Big Data**, the **Internet of Things**, and the proliferation of **sensors**, global Information Technology (IT) giants like ***Microsoft*** and ***Google*** are positioned to process many **zettabytes** of data, enabling them to glean and publicly share insights about the global **DataSphere**.

Smart phones and commercial drones have harnessed and converged this awesome power into the hands of ordinary citizens. In transforming the twenty-first century battlespace — making it increasingly transparent and enabling everyone to be a potential sensor and intelligence asset — it has also blurred the distinction between combatant and non-combatant. This democratization of intelligence also has the potential to erode our Nation's Information Advantage — enabling adversaries, non-state actors, and hostile individuals alike to challenge our narrative regarding future operations — Read on!]

The reduced cost and increased sophistication and access to private technology is facilitating a democratization of intelligence gathering and dissemination capabilities, empowering smaller nations and non-state actors, and ushering in an Operational Environment where battlefields are transparent to all. This exponentially increases the amount of data and information available and the number of entities to whom it is available. Russia's on-going "special military operation" in Ukraine serves as a proving ground — testing the limits of this emergent, democratized PED capability and showcasing non-government entities' growing ability to impact conflicts around the globe. Ukraine's willingness to integrate democratically-sourced information, data, and analysis provides a blueprint, allowing nations and non-state actors alike to develop and maintain a capable intelligence enterprise, and possibly increasing the ability of states without formal intelligence sharing agreements to collaborate more effectively. The impact of democratized intelligence on the Operational Environment presents important operational and legal questions for consideration as the U.S. Army continues to successfully compete, deter aggression, and failing that, fight and decisively win future conflicts.

Russian invasion of Ukraine – military offensive starting on 24 February 2022, part of the Russo-Ukrainian War / Source: Image by Viewsridge, via Wikimedia Commons, CC BY-SA 4.0

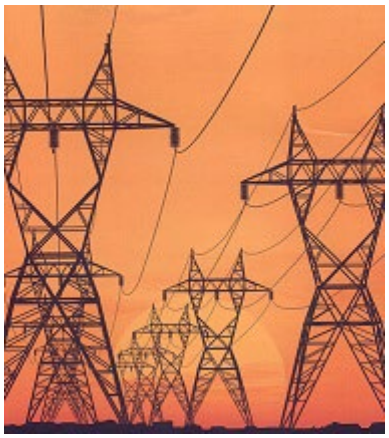
Following Russia's invasion, Ukraine openly solicited commercial imagery, handheld video, voice intercepts and Artificial Intelligence (AI) translation, and satellite imaging to bolster their intelligence capability. In April, for example, Ukrainian law enforcement submitted a cell phone conversation to ***Radio Free Europe***'s Russian Language Service between a **Russian soldier and his wife** where she reportedly gave him permission to rape Ukrainian women — "*Just wear protection.*" Not only did RFE journalists use social media to identify the couple, but the conversation's publication allowed social media users to apply AI language translation for access by wider audiences. ***Primer***, a private AI company, similarly identified Russia's widespread use of **unencrypted communications**, and used its translation programs to create a searchable database of audio transcripts which highlight operationally relevant information. The ***Institute for the Study of War***, a private think tank, uses the commercial WGS 84 Web Mercator tool to display ***MAXAR*** satellite imagery and Ukrainian government reports of military activity on maps shared to social media that depict frequently-updated **areas of fighting** and control in Ukraine. Posts on ***Telegram*** and other social media platforms show photos claiming many Russian aircraft are equipped with insecure, commercial **GPS systems** instead of military navigation equipment. There are also allegations that Russian military

commanders used **cell phones** to issue commands and communications, as opposed to secured radio or communications systems. Ukrainian sources also claimed Russian intelligence agencies are using shell-corporations to purchase **private satellite imagery** that is formally unavailable to the Russian government in order to aid targeting efforts. Ukraine's approach to open-source and publicly collected information exemplifies the ways democratized intelligence can allow any country to establish a capable intelligence enterprise in times of conflict. **Open-Source Intelligence (OSINT) and reporting have aided Ukraine's quick response to the fast-paced modern news-cycle, which has bolstered international support regardless of many nations' lack of formal information sharing agreements with Ukraine.**

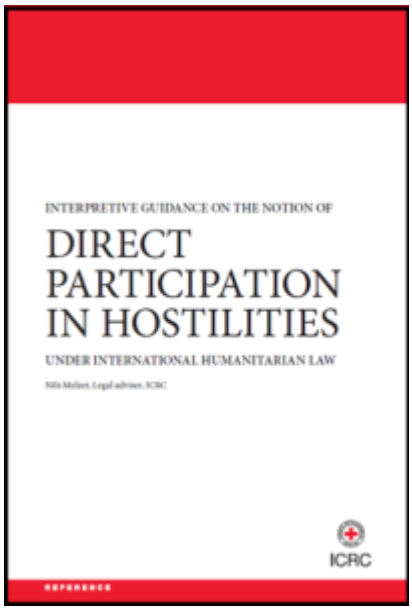
Intelligence production capabilities have also extended beyond well-funded entities in industry and academia. **Ukraine's unprecedented decision to invite private citizens from all over the globe to take part in the fight against Russia has tied its intelligence architecture to the public.** Tech savvy individuals are leveraging technology's dependence on the internet to target infrastructure and impact the conflict on Ukraine's behalf. Unidentified activists were reportedly able to **locate and flip "kill switches"** on 27 tractors stolen by Russian troops and shipped to Chechnya by tracking their embedded GPS signatures through the dealership's database. Similarly, a **15-year old drone hobbyist** in Ukraine used his own drone to help Ukrainian artillery target and destroy a Russian column headed towards Kyiv — an example of the larger ***Facebook***-coordinated effort of Ukrainians with private drones submitting Intelligence, Surveillance, and Reconnaissance (ISR) information to the defense effort. Ukrainian app developers and programmers have created *ad hoc* digital infrastructures that allow civilians to document **war crimes**, contribute to **cyber attacks** on Russian military websites, and **report** location-tagged photos and videos of Russian troops directly to Ukrainian intelligence agencies. According to Ukraine's Minister for Digital Transformation **Mykhailo Fedorov**, these sites receive tens of thousands of submissions per day and are used by Ukrainian intelligence officials to coordinate defense and counterstrikes. Crowdsourced information has also aided in the development of Ukraine's "**Book of Torturers**" database, which publishes the identities and alleged war crimes of individual Russian soldiers. **These individuals' capacity to informally volunteer their services to influence the conflict signal future conflicts where such civilian capabilities will continue to expand with technology and complicate Service members' ability to distinguish between combatants and non-combatants.**

Examples of democratized intelligence capabilities from the Russia-Ukraine conflict indicate both opportunities and challenges for the U.S. Army. **Individuals' growing**

ability to influence and even disrupt technology may jeopardize the integrity of the information gathering infrastructure that the U.S. Army depends on. Such capabilities may also blur the lines between combatant and non-combatant actions on the battlefield. The remote disabling of stolen tractors and similar reports presage a future where "hactivists" can target and disrupt a nation's vital **infrastructure** (e.g., power grid, water, and hospitals) or even impact its ability to produce and distribute key commodities (e.g., fuel and food). While Ukraine's open dialogue with the global commons demonstrates crowdsourcing opportunities for intelligence gathering and promoting favorable narratives in a future conflict, **it conversely illustrates that the U.S. Army may not be able to limit non-military actors' extensive documentation of future battlefield operations.** Similarly, social media platforms could be used to support deception efforts, like posting misleading information about the potential destination of troops and equipment. Conversely, good-faith independent fact-checkers could investigate and publicly counter the authenticity of attempts to misdirect or deceive an enemy's detection of U.S. troop movements or intent.



The recent war crimes trial of a **Russian soldier** in Ukraine could set precedent for individual soldiers' liability for actions on the battlefield and begs the question regarding whether current definitions of direct participation adequately address the capability technology grants individuals. **Deciding whether to operationalize greater amounts of privately collected and shared information also begs the legal question of whether using such information makes the source a direct participant in the conflict.** Testimony in the trial established that the Russian soldier shot and killed a civilian on his commander's orders because the commander believed that the civilian was using a cell phone to give away Russian troop locations. According to the **2009 Red Cross Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law**, "*an unarmed civilian sitting in a restaurant using a radio or mobile phone to transmit tactical targeting intelligence to an attacking air force would probably have to be regarded as directly participating in hostilities.*" There may have been reasonable belief that the civilian constituted a legitimate target.



Military use of civilian-sourced imagery or data is a logical continuation of this definition, which means that the sources' legal status could potentially change to combatant, whether they are aware of this or not. This is especially relevant when considering the Ukrainian military's use and publication of information collected and submitted by individuals like drone hobbyists, regardless of the good-faith reasons for these actions. For corporations whose infrastructure collects information for a military, this

could mean that an adversary may argue that this infrastructure is a legitimate target. A military's choice to operationalize democratically produced and shared information also indicates a clear moral obligation to inform those information sources that they may potentially lose their protections as noncombatants. The war crimes investigations occurring in Ukraine largely depend on **private investigators**' collection of battlefield information and **facial recognition technology**, which demonstrates the high level of scrutiny already possible. Efforts like the Ukrainian government's "Book of Torturers" are powerful in promoting Ukraine's narrative about the brutality of Russian troops, and could reinforce an expectation for similar public databases in the future, whether by a government or private entities with lower standards for accuracy. **In a future conflict, a U.S. Army Soldier's every move could potentially be documented in theater – accurately or not – and posted by bystanders, which could then be nefariously used by an adversary to gain information advantage and erode both domestic and international trust in our operational narrative.**

Because modern technology allows non-military actors entry into a military's intelligence process, an adversary could potentially argue that this implicates these entities in the kill-chain, possibly making them legitimate targets. Conversely, the U.S. Army may find it difficult to determine what is and is not a legitimate target during hostilities. **Examining the on-going conflict in Ukraine could aid in developing standard practices for mitigating threats from non-military actors collecting or disseminating information without reacting to them as formal combatants.** Defining the role and limits of democratized intelligence capabilities can produce clear operational and legal definitions that strike a balance between protected action and direct participation. Adapting to the opportunities and addressing the challenges posed by democratized intelligence well before the U.S. Army's next conflict can facilitate policy development that protects both Soldiers and private entities, while preserving the spectrum of responses to possible adversarial actions in the Operational Environment — where any and everyone has the potential to influence future conflicts.

If you enjoyed this post, check out Kate Kilgore's previous post -- **Russia-Ukraine Conflict: Sign Post to the Future (Part 1)**

... as well as the following related content:

Space: Challenges and Opportunities

Nowhere to Hide: Information Exploitation and Sanitization and **War Laid Bare**, by **Matthew Ader**

Integrated Sensors: The Critical Element in Future Complex Environment Warfare, by **Dr. Richard Nabors**

Warfare in the Parallel Cambrian Age, by **Chris O'Connor**

The Future of War is Cyber! by **CPT Casey Igo** and **CPT Christian Turley**

In the Crosshairs: U.S. Homeland Infrastructure Threats

China and Russia: Achieving Decision Dominance and Information Advantage by **Ian Sullivan**, along with the **comprehensive paper** from which it was excerpted

The Erosion of National Will – Implications for the Future Strategist, by **Dr. Nick Marsella**

About the Author: ***Kate Kilgore*** *is a TRADOC G-2 Intern and recent graduate of Indiana University, where she studied Law and Public Policy, Comparative International Politics, Soviet History, and Russian and Eastern European Studies. Kate has been greatly influenced by her father's Army career, and she grew up all over the United States and in Germany, which influenced her passion for Eastern European history. Much of her undergraduate research focused on analyzing the path dependence and modern social implications of Soviet laws and in the former Eastern Bloc, with a focus on Hungary. When she's not reading about culture and politics of the former Warsaw Pact States, she enjoys baking and antiquing.*

Disclaimer: *The views expressed in this blog post do not necessarily reflect those of the U.S. Department of Defense, Department of the Army, Army Futures Command (AFC), or Training and Doctrine Command (TRADOC).*