Data As A Weapon: Psychological Operations In The Age Of Irregular Information Threats

Description

This Irregular Warfare Initiative article was originally posted through our partner organization, the Modern War Institute at West Point.

Russiaâ??s invasion of Ukraine is arguably the first war to be documented and fought on social media. At the beginning of the war, Ukraine seized the initiative in the information environment, which helped Ukraine garner significant international support. Domestically, social media content, like the video of a Ukrainian farmer stealing a Russian tank with his tractor, has boosted Ukrainian morale. But these messages compete for influence in a space full of unprecedented amounts of content and disinformation. Making sense of, and creating advantages from, this deluge of information is a strategic imperative for any modern military.

A few weeks prior to the invasion, Secretary of the Army Christine Wormuth outlined her priorities for the US Army in a letter to the force, underlining the pivot toward great power competition with Russia and China, and the massive digital modernization required to face this threat. Her second priority highlighted the need to upgrade the US Armyâ??s data and network capabilities to maintain its advantage in contested areas. This is because the information environment is increasingly complex and important for the cognitive aspect of conflict. If the US Army hopes to deliver decisive effects in the information environment, it must modernize the capabilities of psychological operations (PSYOP) units, which are designed to operate in this space against both near-peer adversaries and irregular threats.

Constrained and Unconstrained Information Environments

American PSYOP units are still primed to use the planning processes of past wars, when radio broadcasts, leaflets, and handbills were the primary means to communicate with target populations. These methods work well only within constrained information environmentsâ??low-resource settings with scarce telecommunications infrastructure and low internet penetration rates. For example, ISIS created such an environment with its ban on private and WiFi-enabled internet. As a result, traditional PSYOP methods like leaflets were effective because only ISIS and coalition narratives were vying for influence.

But US adversaries often operate in unconstrained information environments that are highly contested, enabled with high internet access, and filled with effectively unlimited media narratives and sources. Just outside of ISIS-controlled areas, we found, in our experience conducting and leading PSYOP operations, that the same PSYOP teams were dramatically less effective because they lacked the analytical capabilities to truly contest an unconstrained information environment.

US PSYOP teams in Somalia performed similarly. The rural areas were highly constrained due to low literacy, low internet penetration, and the confiscation of smartphones by antigovernment forces. The Somali National Army and US teams performed well in these areas by communicating through handbills, posters, stickers, and leaflets, heavy with explanatory imagery. In contrast, PSYOP teams struggled in urban areas, where the information environment was unconstrained, consisting of mixed media via high internet access, television, radio, and traditional news media. Both Somalia and Iraq demonstrate that a variety of environments exist in close proximity to each other and that PSYOP units need to understand them at a granular level if they are to wield influence effectively.

First-Mover Advantages

PSYOPâ??s main outputâ??influenceâ??relies on the ability to collect information, analyze it, and rapidly exploit the information environment. This is increasingly difficult in unconstrained environments, where adversaries have access to more advanced data aggregation, monitoring capabilities, and effective use of social media. Russia and China excel in this regard.

But analysis alone is not enough; speed matters too. The competition for influence has a distinct first-mover advantage. Research shows that simply countering fake news with accurate information is not entirely effective due to cognitive bias and the misinformation effect, whereby bad information can change peopleâ??s perceptions of past events. It is therefore critical to engage with adversarial narratives before they gain traction, which can generate credibility, especially when corroborated by outside observers.

These dynamics are currently playing out in Ukraine. Russiaâ??s information warfare campaign relies on both state-sponsored networks and covert channels to spread disinformation. Information warfare, propaganda, and cyberattacks against Ukrainian infrastructure are meant to break Ukraineâ??s will to fight. Internally, Russia is targeting its citizens by blocking Western social media and news platforms while simultaneously pushing pro-invasion propaganda. This has created a constrained information environment and has further divided the country between those who rely on state-sponsored media and those who use VPNs and other methods to circumvent censorship.

Surprisingly, Russiaâ??s external disinformation efforts have been largely ineffective because Ukrainian messages are transmitted quickly and target allied populations already skeptical of Russian media. Ukraineâ??s social media campaigns have enlisted international and domestic support, by showing civilian harm and mythologizing heroesâ??whether real or exaggeratedâ??like the Ghost of Kyiv and the soldiers of Snake Island. Additionally, the United States, Ukraine, and other Western powers successfully prebunked Russian disinformation by releasing intelligence regarding Russian operations before they occurred. In aggregate these campaigns enabled Ukrainian messaging to dominate Western opinion and have been decisive in eliciting foreign military aid.

To fully counter information threats, the PSYOP community must gain a similar first-mover advantage in both constrained and unconstrained environments. Active anticipation, identification, and engagement with narratives as they emerge is a critical component of effective PSYOP, but to do this in an unconstrained information environment requires significant improvements to collection and analytic capabilities.

What Does PSYOP Modernization Look Like?

The PSYOP community must modernize to rapidly understand the information environment and effectively influence target populations. PSYOP begins with collection and analysis to â??sense and make senseâ?• of the information environment, but the Armyâ??s doctrinal processes leave PSYOP as a low priority due to their focus on kinetic threats. This limitation can be overcome, in part, by investing in more access to publicly available information, such as modern network architecture that can ingest and warehouse such data. Then, making sense of the environment requires improved capabilities to exploit data with automated processes, software tools, and skill training.

To be sure, there are many top-down efforts guided by the 2019 Army Modernization Strategy and the DoD Artificial Intelligence Education Strategy to generate a force capable of multidomain operations. Key efforts include the Army Futures Command Software Factory, which provides training for software developers and platform engineers, and Army Intelligence and Security Commandâ??s Cyber Military Intelligence Group, which aims to exploit complex information environments. These efforts are critical, but the Army also needs bottom-up innovation at each level. What follows are some recommendations, but a diverse range of expertise is needed to identify the pain points at every level of the organization and propose corresponding solutions.

The Team Levelâ??Field More Automated Tech

With improved capabilities, a standard twelve-soldier PSYOP detachment could iterate on approved campaigns in real time and produce more decisive effects. In an unconstrained environment, the digital

complexity of social media can only be adequately exploited using automated processes. A standard algorithmic toolkit might include language-translation tools, multimodal algorithms to process memes and videos, social media API scraping tools, and unfettered access to open-source news and publicly available datasets. In constrained information environments, PSYOP teams need tools that support language translation, optical character recognition for translating written or newspaper text, and speech-to-text translation. These capabilities would allow for quick insights into the target audience without the constant need for trained linguists. Commercial artificial intelligence is already transcribing and translating the Russian armyâ??s unsecure radio broadcasts in Ukraine.

The Plannersâ??Develop Dashboards with Broad Capabilities

PSYOP planners conducting initial target audience analysis can benefit from a standardized dashboard with livestream information on trending social media topics, event-based alerts, and audio-to-text machine translation. Fielded software solutions might encompass a mix of different commercial off-the-shelf software or the acquisition of larger software standardized across the force to automate many manual tasks and enable better anticipation and identification of emerging narratives. Such a toolkit could be used across the spectrum of information environments.

The Community Levelâ??Accept Risk to Acquire Technical Skills

In conjunction with technical upgrades, the PSYOP community needs soldiers with technical competence, but training often creates short-term risk for commanders through personnel gaps and financial costs. Fortunately, some training paths have already been pioneered, such as the Joint Special Operations Commandâ??s data literacy pipeline, which sends participants to industry for three months of training. This program ensures a return on investment by selecting only motivated and technically competent personnel. Alternatively, data bootcamps, such as Code Academy, provide flexible content delivery and are a fraction of the cost of a traditional advanced degree. Data skills that go beyond widely available commercial platforms are important to develop more agile PSYOP campaigns in all environments.

All upskilling approaches also require a follow-on plan for integrating soldiers into roles where they may use these skills, ideally on a team that can provide more in-depth on-the-job training and domain knowledge. Finally, all of these initiatives create a climate in which soldiers are encouraged to â??fail fast and learn fastâ?• because technical skill and innovation are rewarded.

Competing in a Data-Driven World

The information environment is decisive terrain for modern combat. It is characterized by increasing complexity, and analysis and speed are the key drivers to successfully influence target populations. Current doctrine and processes are effective in uncontested information environments; they offer few answers for a social media-driven world. The PSYOP community must modernize its capabilities, which is not a protracted, multibillion-dollar process. Rather, it requires exploitation of publicly available information, skill training, automated and machine learningâ??aided workflows, and software solutions. Moreover, PSYOP modernization will enable multiple warfighting functions, including intelligence, mission command, and sustainment. As the secretary of the Armyâ??s message to the force made clear, data modernization is critical for the United States to remain competitive against hostile state actors.

Jon Reisher is a masterâ??s student at Carnegie Mellon Universityâ??s Heinz College pursuing a degree in public policy and management. He is also an active duty PSYOP major with multiple deployments to Afghanistan, Iraq, and the Middle East.

Charity Jacobs is a PhD candidate at the School of Computer Science at Carnegie Mellon University, a data scientist with the Department of Defense, and a military intelligence major with the US Army Reserve. Her research interests include applied machine learning, natural language processing, and disinformation detection.

John Beasley holds a master of business administration from the Johnson Graduate School of Management at Cornell University. He is also an FA30 (information operations) major with the US Army Reserve with multiple deployments to Afghanistan and East Africa.

The views expressed are those of the authors and do not reflect the official position of the United States Military Academy, Department of the Army, or Department of Defense.

Image credit: Esercito Italiano, via Wikimedia Commons

Date Created
2022/05/02