Hiding In The Noise: Preparing The Irregular Warfare Community For The Age Of AI

Description

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

According to the 2020 Irregular Warfare Annex to the National Defense Strategy, the United States is underprepared to counter irregular warfare; the dawn of the AI age compounds this problem. As AI continues to transform human society by fundamentally changing how people experience reality, US adversaries are already using it to augment their forces, conventional and unconventional alike.

To win, the United States will need to both combat AI-enabled adversaries and find creative ways to get its forces running at machine speed using AI. To effectively conduct irregular warfare in the AI age, the US military must adapt its doctrine and training to address these AI-enabled threats.

AI Has Already Changed Irregular Warfare

The AI age is here, and the technologies associated with it are already making it harder to conduct irregular warfare. China has outpaced current US ability to integrate defense and AI by coercing civilian companies to develop dual-use technologies through â??military-civil fusion.â?• As the US Department of Defense makes critical bets on how it will support a high-tech conventional war with emerging technologies that do not yet exist, the US irregular warfare community is already feeling the impact of AI in the competition phase. AI-enabled facial recognition technology, for example, has affected the intelligence communityâ??s ability to protect informants, challenging one of its core competencies.

Seasoned irregular warriors like former commander of US Army Special Operations Command Lieutenant General (Ret.) Charles Cleveland have observed that the advent of AI provides new avenues for irregular warfare. Special Operations Command efforts to bring more data to the warfighter through Project Maven and similar plans demonstrate a willingness to adapt in ways the special operations forces (SOF) community prides itself on, but most meaningful steps toward integrating AI into special operations remain years away. Although new AI-enabled tools, like Project Maven, have the potential to improve SOF operations, practitioners must understand that they cannot sit and wait for these tools to arrive. The SOF community must concentrate on changing its current tactics, techniques,

and procedures to account for how adversaries are already using AI to counter irregular warfare activities.

Adversarial Artificial Intelligence

The most easily recognizable subset of AI is machine learning (ML), which uses mathematical modeling to draw connections in large data sets at speeds impossible for humans to replicate. People experience this every day within tools like Google Maps. ML models are built on the assumption that the training data is accurate, and this assumption can be exploited through â??data poisoning.â?• By corrupting the data ML algorithms use to learn, data poisoning can prevent these algorithms from working properly.

Researchers from UC Berkeley are working on a specific type of data poisoningâ??the â??backdoor attackâ?•â??that requires no knowledge of the underlying algorithm, only access to the databases controlling the training data. With only fifty poisoned training examples, they were able to defeat a facial recognition deep learning algorithm. Data poisoning is only one of several adversarial techniques that can attack AI systems in ways analogous to existing irregular warfare practices. The difference between these and other cyberattacks will be indistinguishable to most practitioners, but understanding their different effects is essential to operational success.

Adding Information Systems to the Targeting Cycle

Allied commandos in World War II did not need PhDs in nuclear fusion to successfully sabotage the German atomic programâ??s most critical facility. Similarly, a PhD in Bayesian statistics is not required to understand how existing ML algorithms might be stopped. Since the days of the Office of Strategic Services, SOF have been using concepts like CARVER to sabotage complicated technology. The United States needs a new digital CARVER matrix today.

One way to help SOF adapt to AI is to start treating information systems as just thatâ??an ecosystem that contains sensors, servers, people, and algorithms. Mapping AI-enabled information systems in this way will enable practitioners to better visualize the system, transforming it into something easily digestible. This digital terrain analysis will help SOF identify, avoid, and, if possible, exploit these technologies when properly incorporated into the intelligence planning process.

Although targeting command and control systems is a time-honored tradition, the new ways in which data, technology, and algorithms work have outpaced doctrine and cultural understanding of how these modern systems function. Russian forces learned this lesson the hard way when their commanders destroyed the Ukrainian 3G and 4G towers needed to run their encrypted Era communication systems,

a critical mistake that forced them to report flag officer casualties on unsecure cell phones. The F3EAD cycleâ??find, fix, finish, exploit, analyze, disseminateâ??should incorporate information systems to compel practitioners to consider these factors, especially in the competition phase. Tactical units should prioritize efforts to increase their competency targeting AI systems, and these skills should be tested through partnerships with industry and the intelligence community.

Adversarial Artificial Intelligence as a Cyber Irregular Warfare Operation

The horrors of an AI-enabled police state are on display in places like Xinjiang, and China is selling this same AI to build a network throughout Southeast Asia, the Middle East, and Africa via the Belt and Road Initiative. These efforts contest the United Statesâ?? ability to conduct irregular warfare, making it more difficult and more expensive. SOF can use AI to undermine government surveillance and support resistance movements. Adversarial AI, for example, is an offensive cyber operation that could accomplish this task and shape the battlefield by generating temporary glitches that allow operators freedom to maneuver in a highly surveilled environment. SOF practitioners may also find human analog hacks to be effective, through practices like changing outfits and deliberately fooling deep learning algorithms with irregular markings. Taking these precautionary measures will be essential to most irregular warfare operationsâ?? future success.

Capable advisors can also help local forces use open-source ML tools that are readily available online. Using organizations like Bellingcat as models for collecting intelligence to support resistance movements, Green Berets and other practitioners can leverage these widely available tools and technologies to provide comprehensive support to allies standing up to techno-authoritarian entities. Protestors in Hong Kong, for example, were able to combat Chinese facial recognition technologies with laser pointers.

The ability to defeat enemy information systems does not lose its relevance as warfare transitions to the conflict phase. Practitioners will have to put adversarial systems offline to allow for freedom of maneuver, and such efforts will become a modern form of traditional sabotage operations. There are ample opportunities for ML algorithms to fight other ML algorithms in an operational context. For example, data poisoning techniques used to shape an operation may be sniffed out by enemy algorithms that will adjust after detecting deception methods. How adversarial algorithms adapt to the techniques the United States employs, and vice versa, will be a constant concern in all stages of conflict going forward.

Changing the Culture with SOF Operators

US special operations forces have already made great strides in understanding cyber, specifically how to reduce digital signatures during operations, but a similar approach will not be enough to sufficiently integrate AI into these forces. Although AI is accessed in the cyber domain, it is important to clarify that it is not cyber. Instead, its impact will be felt most at the intersection of intelligence and operations. This makes AI inherently different and more difficult to comprehend, and the average practitioner will need to understand it more completely than they currently understand cyber. If SOF operators continue to deal with cyber by holding up burner phones and virtual private networks as magical talismans that protect them from the new digital mages, they will remain unprepared for operations in theaters with AI systems. US Special Operations Command should consider adding courses that equip leaders and planners to identify and beat rival information systems in an operational context.

In order to be effective in this space, the US military must change how it thinks about its operating environments, which requires integrating digital exhaust training into all exercises. This will help those on the ground better visualize how adversaries use their data against them and will create a culture that understands the importance of AI and how it can work for them. It will also help translate what operating in this new environment looks like for the experienced combat veteran who is well versed in irregular warfare but reluctant to adapt to the rapidly changing technologies that now permeate the operational space. And it will give operators a distinct advantage as the United States integrates its own AI tools into its intelligence and operations processes, as they will already be familiar with the benefits and vulnerabilities of AI.

Irregular Warfare in the AI Age

Machine learning and big data can improve how the SOF community conducts irregular warfare operations at scale. More data will allow SOF practitioners to better support resistance movements around the globe. However, these efforts will take time and require dedicated leaders who prioritize integrating data scientists and cyber practitioners into the force in a meaningful capacity. The world economy is only getting more addicted to data, and US adversaries are using this to advance new forms of authoritarian governance. The need for irregular warfare will increase as these tools make conventional warfare harder to conduct. Irregular warfare operators will have to learn to hide in the noise to defeat these new instruments of power. By adapting its doctrine, training, and mindset, the US military can ensure that it is ready to operate and engage its enemies *now* in the competition space.

Captain Matthew Moellering is currently in the second cohort of Army Artificial Intelligence Scholars at Carnegie Mellon University. He is pursuing a Master of Information Systems Management / Business Intelligence and Data Analytics from Heinz College. He is a Special Forces officer with deployments to the Middle East and Afghanistan.

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

Date Created
2022/09/26