11 July 2023

PERSPECTIVES

The Newest Weapon in Irregular Warfare – Artificial Intelligence

By Mohamad Mirghahari

On the morning of 22 May, 2023, an artificial intelligence (AI) generated image of an explosion at the Pentagon surfaced online and spread like wildfire throughout social media. Multiple news sources reported and shared the AI-generated image on their platforms. As a result, markets responded to the reports and image, and the S&P 500 index fell in just minutes after its reporting, causing a $500 billion market cap swing, even though this image was quickly proven as fake.

Artificial intelligence provides an ever-expanding set of new tools that can be applied in irregular warfare, from targeted disinformation campaigns to military deception (MILDEC). In 2012, a Department of Defense (DoD) Joint Publication defined MILDEC as content "intended to deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action." The Pentagon deep fake (or AI-generated image), which served to negatively impact the U.S. economy and create a substantial amount of confused and misleading reporting, demonstrates that this technology can be used for military deception purposes.

By using artificial intelligence to create different mediums for influence, one can potentially create the illusion of an ongoing war, an attack, a resistance movement, and other versions of collateral for information operations. This use of AI can meet the goals of MILDEC as defined by the DoD.

The image of the explosion at the Pentagon is just the tip of the iceberg of how AI could be used not only to drive disinformation, but also to conduct economic sabotage. Across multiple domains, AI can be an essential part of achieving the objectives of any military operation.

AI can also be used to directly support irregular warfare, such as cyber and influence operations, in a number of ways, both strategically and tactically.

For example, AI can support military deception by automating the creation and dissemination of disinformation, thus removing its development from the hands of planners and teams required to build influence campaigns, leading to increased dissemination of disinformation or messages. Conventional wisdom suggests that increasing the rate of message output or utilizing highly visible entities as amplifiers (such as celebrity "influencers") would help to attract a "stickiness" factor to the message being disseminated, making it more contagious and thus having a more lasting impact, an idea popularized in Malcolm Gladwell's book *The Tipping Point*.

Beyond conventional approaches, artificial intelligence, when coupled with algorithms designed to influence targeted audiences, can generate realistic fake news, social media posts, and other content that manipulates public opinion, confuses adversaries, creates negative or positive sentiment, influences networks, or diverts a population's attention at a pace which will make it difficult for governments, military forces, and news outlets to verify or confirm an image or recording is fake.

AI can tailor disinformation campaigns to specific target audiences, making them more effective from a macro to micro level. AI can maximize information operations support to irregular warfare by analyzing large amounts of data, including social media, to identify target audiences, understand people's psychological profiles, and tailor persuasive messages accordingly. AI algorithms can also improve and synchronize content and delivery of these messages to maximize their impact on the target audience.

For example, a demonstration from a private network science and machine learning company FNA isolated which 20 specific international media personalities could best drive down Russian sentiment in Mali, thus lowering the opinion and optics of the Malian people towards Russia and its activities in Mali. These 20 personalities were, by name, identified out of more than 10,000 potential influencers for this activity within just a few minutes, and could even be further filtered based on their network proximity to specific target audiences. However, the inverse of this result is also true: these same 20 personalities are also the accounts to suppress, overwhelm with traffic, or otherwise degrade to achieve the opposite effect, which is to avoid changing Malians' sentiments on Russia despite Wagner operations in the country, which are suspected to have included massacres and summary executions of the local population.

These solutions, difficult and time consuming to devise from traditional means, utilize different faces of AI, including combining network science features and natural language processing into different machine learning models. The target audiences and the best people to influence the audiences are automatically identified by AI-driven processes, and can be further tuned (or, reinforced) to achieve more specific or greater results over time. A process like this could determine whether you are part of an influence campaign or separated into an echo chamber. The content you consume could have been first generated from an AI deep fake set of images, like the Pentagon attack images from 22 May 2023—a one-two punch not only designed to create a deceptive set of contents, but also to specifically influence or not influence you to contend with the spread of false information.

In planning and during phase zero and one operations, deep fake AI technology can be used to fabricate realistic audio, video, or images to shape the battlefield. State and non-state actors have already been employing the use of this technology. The Venezuelan government has been using AI deep fake technology acting as American newscasters to spread disinformation, and the same AI technology used by Venezuela was also used to spread propaganda in China and Burkina Faso.

Deep fakes can be used to create false evidence, misleading videos, or fake personas to confuse adversaries or manipulate their decision-making processes. These AI-generated deep fakes can be used to draw out desired opponent reactions to an event or policy.

As illustrated by the photo of the alleged Pentagon explosion, by the time the image was declared fake, the intended effects had taken place, including the economic impact and quite likely a security posture change. In addition, emergency services within proximity of the Pentagon shared statements countering the social media reports of the explosion.

AI can help commanders lure and attract adversaries by analyzing their behavior, creating intelligent decoys that look like real targets, generating false communications, and other targeting information used to disrupt their planning. AI can also create false signaling and messaging through AI-developed communications. From AI-generated radar transmissions to communication transmissions such as text messages, phone calls, and radio communications, AI can be used to confound enemies and hinder their decision-making.

As shown by the S&P fall with the "news" of an explosion at the Pentagon, AI can be leveraged for an even more dangerous role in irregular warfare: economic sabotage. AI algorithms can be used to manipulate financial markets, destabilize economies, or undermine confidence in currencies. AI systems can analyze market trends, news sentiment, and social media data to predict and exploit weaknesses in financial systems. They may engage in high-frequency trading, spread false information, or engage in other manipulative practices that cause market volatility or economic instability. Or, in an even more simple way, it can create an image, video, or report that drives the markets down, causing uncertainty in a local economy.

The sectors impacted would not be limited to just the economy. From food security, medical readiness, to supply chain logistics, AI coupled with disinformation can create destabilization in a local populace from thousands of miles away. Could a coordinated information operation use AI and disinformation to cause riots over projected food shortages? How about medicine being restricted in certain areas? Reports of gasoline and oil shortages for the winter? AI can push these narratives at a pace that could shape irregular warfare in ways that we have not seen before.

AI tools such as ChatGPT and Google Bard are becoming more accessible and advanced and will only improve from their current state. The DoD should leverage these tools and build an understanding of how to use them in irregular warfare both offensively and defensively. While it is true that deep fake and AI technologies are constantly improving, it is also the case that tools to counter it have been rapidly growing as well. Some of the most advanced and life-like deepfakes are created by having two AI algorithms working against each other in Generative Adversarial Networks (GANs). As a result, these same techniques can be used to develop algorithms for both creation and detection.

The Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO) overseas the DoD's adoption of data, analytics, and AI to generate decision advantage. While this initiative looks at the AI issues at a higher level, the establishment of DoD AI teams at the command and tactical levels are necessary to monitor information flow and AI-related content. This would allow the DoD to study trends and effects from state and non-state actors both tactically and strategically. Additionally, it would facilitate the DoD use of AI at both a command and tactical level to shape messaging on the battlefield, coordinate information operations at an increased frequency, and potentially counteract any counter-AI related disinformation or content related to ongoing operations.

About the Author:

Mohamad Mirghahari is the National Security Fellow at Seton Hall University's School of Diplomacy and International Relations. Mirghahari previously served in the Department of Defense in key leadership positions, in support of counterterrorism and Special Operations initiatives that have significantly impacted mission-critical outcomes across the globe.

Disclaimer: This IWC Perspectives article reflects the views of the authors and are not necessarily the official policy of the United States, Germany, or any other governments.