

The info war is as much about ideas and perception as it is about data





U.S. Army Lt. Col. Jason Welch, United States Indo-Pacific Command, asks a question during the Artificial Intelligence (A.I.) systems for Public Affairs brief, at the Public Affairs Leadership Development Forum (PALDF), in the Hyatt Regency Waikiki Resort Conference Room, Mar. 31, 2026. (U.S. Army Photo by Sgt. Qishaunia Hawkins)

Being able to tell the commander you don't need to do something is actually a powerful message, as well

By **BREAKING DEFENSE**

Information warfare is nothing new. What is new is the addition of social media and artificial intelligence (AI) making it possible to spread dis- and misinformation faster than ever, necessitating a rapid response to help maintain parity in the information battlespace.

Look no further than the Iran conflict, which has spawned a network of AI-generated videos claiming to be US servicemen and women. The University of Southern California's Information Sciences Institute identified a network of more than 100 TikTok accounts impersonating US personnel, with more than 3 million views and 440,000 engagements on videos ranging from "soldiers" claiming to be distressed to asking for support for their mission.

There are numerous other forms of modern-day information warfare as well, from mocking and taunting such as Iran's videos of US administration officials as Lego figures to propaganda in the Ukraine conflict. Being able to respond to a varied range of what has effectively become meme warfare necessitates quickly identifying target audiences, formulating the right message and determining the best way to get it in front of people, explained Bobby Muscara, associate director for Europe at Two Six Technologies, who is in the trenches with the company's partners that depend on cutting-edge technologies to complete their missions.

"We have analysts who do routine threat analysis in the information environment, and what we've seen from both



On the cover: A U.S. Marine with Joint Task Force-Ares introduces Ryan McBeth, an open-source intelligence analyst and cybersecurity expert, before a professional military education session at Fort George G. Meade, Maryland, July 23, 2026. (U.S. Marine Corps photo by Sgt. Isaiah W. Smith)



U.S. Army Warrant Officer 1 Gabriel Lucero, cyber warfare technician, instructs members of the Botswana Defence Force and Botswana cyber professionals on defensive cybersecurity practices during Exercise Southern Accord 2026 at Gaborone Technical College in Gaborone, Botswana, August 11, 2026. (U.S. Air National Guard photo by Staff Sgt. Reanna Hartgrove)

Russia and China is that they're using AI and large language models (LLMs) to enhance their information operations campaigns," Muscara said. "Whether it's multiple languages – Russia, for example, was using two a few years ago, and now they're up to six languages for the majority of their propaganda – and China is increasingly disseminating their propaganda in English and other languages. Other adversaries use AI as well. Iran, as we've seen recently with their 'Lego' videos. Our clients need to be able to react fast to those narratives the adversaries are pushing out and disseminate content as fast as possible."

Winning on the information battlefield means being able to attack and counterattack quickly, with messaging that is compelling to the people who need to hear it. That isn't as simple as dropping leaflets or radio broadcasts anymore. The tools have changed quickly, and understanding and using them effectively is critical to success.

The US military is embracing this challenge, as multiple branches have recently announced new initiatives or changes in how they conduct information warfare. In late 2025, the Navy launched a pilot program to incorporate information warfare squadrons within carrier groups and the Army announced it was adding electronic warfare and information advantage to the responsibilities of its principal cyber advisor.

In July, the Marine Corps announced that it is working on an information warfare plan that will encompass the entire Corps, building a framework that will encompass training, funding requests and sharing information with industry representatives to identify the information warfare tools the Corps needs.

"There is an insatiable demand and realization by combatant commanders now that non-kinetic effects are integral to what they need to do, and they are turning to the services, particularly to the Marine Corps, to say, 'Hey, I need this capability in addition to the traditional arms of the'" Marine Air-Ground Task Forces, Deputy Commandant for Information Lt. Gen. Joseph Matos said at the Modern Day Marine Conference in April. "Those demand signals are out there because they realize, in order for the combat commander to do his job, they need these non-kinetic effects from across the services."

AI tools are providing new information warfare capabilities that demand immediate, trustworthy responses. Deepfakes and misinformation campaigns aim to not only control the narrative on the battlefield, but destabilize governments or sway public opinion. While fighting on the battlefield may be contained to one region, the narrative surrounding it has no geographic constraints.

"Frontier AI capabilities can be used by potential adversaries to enhance cyber operations, generate convincing disinformation at scale, or support targeting in ways that compress decision timelines and increase escalation risks," Adm. Richard Correll, Commander, STRATCOM said at the Defense Intelligence Agency's 2026 DoDIIS Conference. "The question is not whether AI will be present in the future conflict. It already is."

When a campaign is gaining traction and needs to be countered, a rapid response is critical to effective counter-messaging. Muscara points to three tools: understand the information environment, create the content needed to counter a campaign and disseminate it. Two Six's Sentr – the company's



recently launched agentic AI-driven “command center” for the narrative battlefield – combines all three of those capabilities into one platform, streamlining the process for identifying propaganda, drafting a counter and distributing it effectively.

Using both agentic AI and LLMs, Sentr can scour social media sites and the larger internet to compile data on active campaigns infinitely faster than humans, compile metrics on the effectiveness of those campaigns and track how they are evolving.

Once a counter message is decided on, Sentr can distribute it and track its effectiveness, as well, giving users the ability to modify the message as needed to ensure it is resonating with the target audience. With one platform offering all of the necessary capabilities, Muscara said customers have seen response time cut by 85 percent with Sentr.

“The crucial thing is that we can inject information into the information environment all with one tool, rapidly, without needing to coordinate between three different types of tools or vendors to get after one problem,” he said. “That rapid lifecycle is done in-house in one platform, and that’s how we can enable the customer to rapidly disseminate content.”

Identifying the narrative

With so much information flying around on a daily basis for everyone – regardless of whether they are in a contested or potentially contested area or not – it is hard to separate what is trolling or people making memes for fun versus potentially serious disinformation or misinformation campaigns. Social media apps enable instantaneous sharing of information, both true, false or twisted, but when false information is corrected, the correction often receives much less attention than the original post.

Or, as the old saying goes – often misattributed to Mark Twain – “a lie gets halfway around the world before the truth gets its shoes on.”

The first step to combating the information flow is identifying the core narrative. With so much information being shared so quickly, not everything can be fought against. Sentr gets to the root of the information campaign and compiles the necessary data in

a way that it can be viewed holistically, said Muscara.

“Once we collect that small data lake of curated data that matters to our customers, the AI can rapidly identify those narratives by asking simple prompts such as ‘what narratives is Russia pushing in Lithuania over the last seven days?’ and it’ll bring back language-coded responses showing you what Russia has pushed from all different platforms, as well as citations, so you can go back and look at the original content,” said Muscara. “That’s a way for our customers to rapidly assess the information environment as opposed to going to various websites or social media platforms. It’s all in one place.”



Capt. Gonçalo Atanásio, assigned to the Portuguese Armed Forces, participates in the Capture the Flag event during Cyber Shield 2026 at the Professional Education Center in Little Rock, Ark., July 17, 2026. (U.S. Army National Guard photo by Spc. Brooke Kentler/Released)

When that information is collected, Sentr’s narrative tools identify common patterns, such as wording, hashtags and target audiences. Then, users can craft a counter-narrative to hit those common areas, allowing for an effective messaging campaign to combat the propaganda.

In some cases, the best path of action is inaction. If a narrative isn’t gaining traction, it can be monitored without a counter-messaging campaign that could draw attention to a false narrative. By tracking the volume of the messaging, engagement and popularity, Sentr helps users maximize their bandwidth – both literally and figuratively – by only developing campaigns when necessary.

“Being able to tell the commander you don’t need to do something is actually a pretty powerful message, as well, and our platform can do that,” said Muscara.

Security and reliability

Sentr is a powerful tool for building and implementing campaigns, which means it is potentially dangerous if it can be hacked or otherwise interfered with. Cybersecurity is a primary concern for the company and its users, and beyond that, the potential for AI hallucinations are also top of mind.

Any AI tool is only as good as the information it draws from. Sentr is not working from an off-the-shelf LLM that could have potentially false data. Instead, it uses what the company calls a full-doctrinal backbone, where each job is carried out under defined doctrinal parameters such as where the information is coming from and how it is supported that set standards for



information should be used and how it should be used. The platform also uses a citations tool that provides context and supporting information for the reporting it does on campaigns, their key components and their reach.

The citations tool offers two methods of verification for users to understand where information is coming from. It has a curated knowledge base that shows users which document is being cited and what information is being pulled from that document. It also can cite articles from the internet, in which case it shows the citation and provides links, accompanying images, authors, the original text and any translated text.

“We can actually show you the real content,” said Muscara. “It’s not just citing a law book in its database. It’s showing real-time or near real-time information of the information environment – and the AI can’t hallucinate a web page.”

All of Sentr’s information flows are curated by human experts, who identify relevant information and build relevant context around it to ensure that users are getting the best possible information to build campaigns. Sentr also tracks history and allows users to audit where information originated as users build out their documentation. Every piece of content can be viewed from the same interface, giving a broad perspective on where information came from, how it was collected and supporting citations to help validate it. The platform is designed to include a human in the loop, allowing for independent evaluation and verification of what Sentr is reporting.

Fundamental cybersecurity is part of the platform, as well. Sentr is an unclassified tool, but the company uses the same security protocols as it does for its systems that operate on classified networks. Two-factor authentication is required, and Muscara pointed out that many of the company’s customers are also well-trained in tradecraft for things such as protecting login info



“

Our message to customers and potential customers is this is an enabler for who you already have and the experts that you already have.

— **Bobby Muscara**
*Associate Director for Europe,
Two Six Technologies*

”

that they apply when they are using the platform.

Sentr can also identify potential leaks or cybersecurity issues when it is compiling data. For example, if the platform is searching for a narrative and identifies related information coming from a friendly source, it can flag it as an operation security (OPSEC) issue, said Muscara.

“You can find it by using the broad-based LLM that’s searching the data lake for this news article or tweet or whatever it was,” said Muscara. “Then you can pivot to create an OPSEC plan to mitigate this or suggest additional training or TTPs that we should implement and send out to all soldiers within the unit.”

Winning the information war

Fighting misinformation and disinformation – or even just correcting information that was thought to be true and later turned out to be incorrect or not quite accurate – is a constant challenge. Whether it’s memes that appear harmless on the surface but are subtly pushing a narrative or full-on campaigns aimed at swaying public opinion or destabil-

ization, adversaries are harnessing AI tools to quickly pump out staggering volumes of information that must be analyzed and countered to avoid ceding control of the narrative.

Doing so requires tools that can offer information specialists the ability to identify and counter emerging narratives before they can take root. By providing a single platform that can encompass all aspects of identifying and responding to narratives, Two Six’s Sentr enables human experts to combine their knowledge with AI tools to respond quickly.

“Our message to customers and potential customers is this is an enabler for who you already have and the experts that you already have,” said Muscara. “We’re making our partners faster, more reliable and more impactful within the platform and the information environment.”