An artist's conception of a Chinese hacker launching an attack on Guam military bases. (AI illustration by Gerardo Mena, Army University Press)

Using CamoGPT AI to Build Scenario-Driven Change

The Example of Guam as a Hybrid Attack Target

Lt. Col. John Ringquist, PhD, U.S. Army, Retired

The experimental U.S. Army AI program CamoGPT debuted in 2024 as a program developed in-house by U.S. Army soldiers for members of the Department of Defense (DOD). When first offered, it provided users with the opportunity to explore potential scenarios in an unclassified setting. The resulting scenarios could provide context for multidomain operations planning, future force generation, and areas of potential civil-military collaboration that may otherwise go unnoticed in the data streams of daily operations. Artificial intelligence (AI) could also enable research into hypothetical scenarios that include hybrid or "gray-zone" warfare that could become a component of future conflicts. The risk of attacks against the U.S. domestic infrastructure are rising as Chinese and Russian gray-zone and hybrid warfare approaches demonstrate the capability for state-sponsored terrorists, criminals, and nonstate actors to destroy or degrade key infrastructure resulting in catastrophic impacts on security and the populace.

Cyber Attacks, Hybrid Warfare, and Volt Typhoon

The U.S. domestic infrastructure is exposed to attacks from domestic and foreign actors, through physical, cyber, and insider-threat means. The Cybersecurity and Infrastructure Security Agency (CISA) Advisory Committee warns that with limited exceptions, critical infrastructure and government agencies have not prepared for a contested environment as a result of nation-state conflict.[1] Despite attempts to improve physical protection for key infrastructure and efforts to develop resiliency against cyberattacks, numerous domestic infrastructure nodes remain vulnerable. Some of the most pernicious attacks occur over an extended period and in the background of existing systems, as back doors and malware work to undermine systems security.

China is the suspected or confirmed origin of many cyberattacks against the United States. The persistent attacks have generated discussion that questions if we are engaged in hybrid war with China. It is possible that we are being probed by Chinese state and nonstate actors in preparation for a larger conflict. In 2022, the People's Liberation Army discussed "Multi-Domain Precision Warfare" as a new way to leverage C5ISR by incorporating big data and AI to rapidly identify vulnerabilities in U.S. systems and then combine forces to launch precision strikes against those vulnerabilities.[2] Cyberattacks used to indirectly determine weaknesses are preludes to a greater Chinese effort to destabilize U.S. alliances, degrade capabilities, and create weakness for later exploitation.[3] The Office of the Director of National Intelligence assesses that China would consider "aggressive cyber operations against U.S. critical infrastructure and military assets … to deter U.S. military action by impeding decisionmaking, inducing societal panic, and interfering with deployment of U.S. forces."[4] One of the most significant threats to the United States and its allies that was uncovered already embedded in numerous civilian utilities is the malware delivered by the Chinese hacker group Volt Typhoon. Despite repeated attempts to deny access and FBI successes against Volt Typhoon in early 2024, Volt Typhoon adapted, and its bots continue to exploit legacy systems through unprepared third parties in the United States.[5] The variety of threats to U.S. infrastructure from Volt Typhoon demonstrates the potential for malicious software to cause disruption of critical military systems and supporting civilian logistics networks.

Multiple Chinese hacking groups operate across the world, but Volt Typhoon characterizes an approach that seeks to attack the underprotected fringes of competing states. Volt Typhoon hackers have attacked energy, transportation, water, and wastewater systems in the United States and its territories.[6] One of the affected territories is Guam, the location of key U.S. forces expected to respond to Chinese aggression, especially in the case of an attempted invasion of Taiwan. Destroying or disabling military response capability through a hybrid attack that disables integrated civilian infrastructure, especially power and water, is one scenario

Lt. Col. John Ringquist, U.S. Army, retired, is an instructor in the Department of Joint, Interagency, and Multinational Operations at Fort Leavenworth, Kansas. He holds a PhD from the University of Kansas and an MPPA from the University of Missouri-Saint Louis. During his career, he served as an engineer, foreign area officer, and attaché in multiple assignments. He also taught history at the U.S. Military Academy, West Point, and served as senior defense official in Luanda, Angola.

that ChatGPT has indicated is likely in the lead up to a Chinese invasion of Taiwan. China is developing plans and capabilities to execute hybrid war that leverage emerging technologies and AI to determine the next war's strategies.

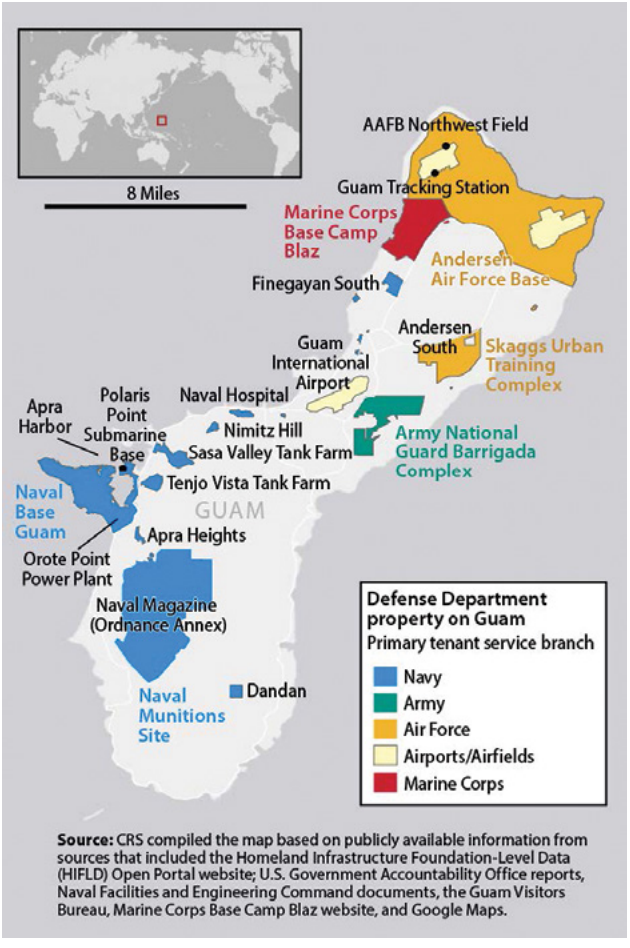
The Chinese army has invested heavily in new technologies as it upgrades its military capabilities. The People's Liberation Army has at least one AI model developed from Meta's Llama model that has been adjusted for military field missions.[7] This model, named ChatBIT, is another aspect of the changing nature of the hybrid battlefield that will be used to identify and exploit weaknesses in opposing forces' conventional forces and support systems. China's military already uses AI for training scenarios, and its joint civil-military programs keep the military intimately engaged in Chinese AI research and development programs. One outcome of the development of AI-enabled technology and dedicated AI models is the opportunity for the Chinese military to continually refine their plans and simulations.[8] The information obtained through multiple sources including nonstate actors, state-sponsored hackers, and espionage ensures data flows to Chinese servers to support AI decision-making for future scenarios. Combating Chinese cyberwarfare will be a major mission for the future but so will training that includes the effects and potential counters to Chinese cyberattacks.

Scenario Development with CamoGPT

Although the use of the AI programs CamoGPT and NIPRGPT were curtailed in early 2025, and the CamoGPT program was restricted by Presidential Executive Order 14271, new AI programs are being considered for the DOD.[9] When it debuted, CamoGPT was an overwhelming success. The enthusiasm for AI within the military is real. The initial promise from using an AI program like CamoGPT to analyze a potential Chinese hybrid warfare scenario against a single node revealed that a large language model (LLM) could select potential targets for the scenario and determine their value and vulnerability. In one example, CamoGPT identified Andersen Air Force Base on Guam as one of the most vulnerable U.S. military bases.[10] A slightly reworded inquiry confirmed Guam as one of the most important bases for a response to a Chinese attack on Taiwan.[11] Further refining opening perimeters for the scenario that did not include a missile attack, CamoGPT AI defined some of the likely targets for a preemptive strike to be Andersen Air Force Base, Naval Base Guam, U.S. military communications and radar facilities, Apra Harbor, and Guam International Airport.[12] Therefore, for this scenario, Guam was separated as a discrete variable from the rest of U.S. Indo-Pacific Command to enable analysis of how a hybrid attack against Guam could affect its ability to support a military and civil response to a Chinese attack elsewhere in the region.

Utilizing CamoGPT for a training scenario that posits a hybrid attack on the island's infrastructure, AI quickly isolated a variety of variables that made Guam vulnerable to Chinese hybrid attacks.[13] CamoGPT selected Guam's critical vulnerabilities and included its remote location, dependence on a single internet provider, and an aging infrastructure including power grid and telecommunications systems vulnerable to distributed denial-of-service attack and ransomware attacks. However, it must be stressed that CamoGPT did make some mistakes, and when we checked the AI analysis, we learned that Guam could be a tougher target for physical infrastructure attacks. For example, Guam has not one but at least three internet providers, and eleven subsea systems and multiple landing stations.[14] The infrastructure analysis was proven valid.[15] The scenario assumed that civilian targets will be struck first across an array of vulnerable cyber and physical infrastructure, and military and government agencies would be targeted by malware. The next steps in the CamoGPT scenario creation and analysis were driven by the need to confirm CamoGPT AI's findings and potential holes in the scenario that could reduce its relevance. Each named vulnerability was assessed, and the CamoGPT scenario was refined by the assessment findings.

Civilian and military sectors in Guam have experienced cyberattacks and are addressing ways to harden Guam against future intrusions. The Guam National Guard has increased its cybersecurity posture and training and collaborates with other military organizations on the island. The Guam National Guard also conducts exercises with U.S. Space Force, and it hosted a cybersecurity summit in 2023.[16] The summit brought together military and civilian representatives to coordinate capabilities and identify solutions to Guam's



(Map by Congressional Research Service)

U.S. Military Installations on Guam

infrastructure issues in the wake of a typhoon that caused extensive damage to communications and other utilities, and the discovery of Chinese Volt Typhoon malware in Guam.[17] Before asking CamoGPT to outline a hypothetical cyberattack, we considered the following factors: solutions were in process, malware was already in the Guam ecosystem, any cyberattack would need to target people via phishing to introduce malware into military and civil systems, and it would require bots making continual efforts to ensure system defeat. This final variable was considered in light of another suspected Volt Typhoon generated series of attacks in 2025.[18] The CamoGPT scenario created via prompts considered these variables.[19] CamoGPT included physical and cyberattacks in its response.

The CamoGPT AI-generated hybrid attack scenario occurred across a multiweek period and recommended several phases, including deception, espionage, and hacking to identify vulnerabilities. Specific steps and methods for an attack have been modified for this forum to prevent adversaries from emulating our findings. At this point we must stress that LLMs require checking, and their recommendations must be weighed against known information and capabilities.

The initial efforts in a hybrid attack could mirror known details of past Volt Typhoon and other similar hacking attacks by employing physical and digital reconnaissance to identify critical infrastructure including the power grid, water treatment plants, and military bases. The readily available Guam online utilities maps and the island's small size can reduce the time required for these options. Some hackers have followed up reconnaissance and networking probing with spear phishing campaigns to target key civil and military personnel. Malware like that used by Volt Typhoon could infect vulnerable systems through a spear phishing attack, then employ a distributed denial-of-service attack to overwhelm Guam's internet infrastructure. The follow-on effort could deploy social engineering messaging (e.g., cognitive warfare to spread disinformation and panic) with bots and human agents amplifying the message. The cyberattacks could then give way to physical attacks against critical infrastructure and military targets to degrade resiliency and destroy key capabilities.

Systems Vulnerabilities and Real-World Developments

The first area of vulnerability against Chinese attack are the computer systems that Volt Typhoon compromised with malware. CISA characterized the Volt Typhoon operations as positioning attempts to allow hackers to disrupt networks in the event of geopolitical tensions or military conflicts.[20] Discovery doesn't guarantee removal and requires continual vigilance. CISA observed that Volt Typhoon was persistent and relied on undiscovered presence in valid accounts. When combined with telecommunications hacks, the potential to compromise massive amounts of data and leave backdoors hidden within computer and telecommunications systems creates an atmosphere of uncertainty and risk. Chinese efforts to compromise U.S. systems continue unabated despite U.S. efforts to destroy networks and hacker groups. The insidious nature of

Several Navy vessels moor in Apra Harbor at U.S. Naval Base Guam on 5 March 2016. The harbor is an important element of the CamoGPT scenario due to its importance for naval operations and reliance on advanced technologies that could become a critical vulnerability if attacked. (Photo courtesy of the U.S. Navy)

the problem is complicated by state sponsorship and China's broad base of nongovernmental and state-sponsored hacking groups. Attacks have expanded to include additional sectors and people that are recognized as legitimate targets during hybrid warfare. Telecom executives, political leaders, and Washington, D.C., insiders have been hacked through similar methods, and as late as November 2024, a Chinese hack of unknown penetration depth and breadth was characterized as the worst telecom hack in U.S. history.[21] Combining a compromise of U.S. leaders' telecommunications systems with a pinpoint cyberattack against Guam would give China the advantage in command-and-control operations during the window of time between the attack and a concerted response from senior policymakers.

Creating a training scenario that can translate into a better appreciation of the vulnerabilities in civilian and military systems requires a way of building the scenario that ensures that the AI model is not the only input to scenario development. Working in an unclassified environment, it is possible to leverage the data that CamoGPT pulls from the internet with the caveat that the program will not provide information that could result in a formula for what exact nodes should be attacked in Guam to defeat the civil-military response. However, for training purposes, analysts can mitigate CamoGPT's shortcomings through research and by applying their own knowledge and experience to the scenario. For example, keeping this scenario within the realm of a short, sharp conflict, the most obvious targets would be military bases, materiel, and support logistics. However, additional targets for sabotage and physical attack are possible for a hybrid attack beyond power substations and water treatment plants. An example of targets that CamoGPT did not identify were the Guam undersea cable and onshoring facilities. The knowledge of follow-on Volt Typhoon attacks in 2025 informed the likelihood that attacks of a similar nature would feature in a future hybrid attack.

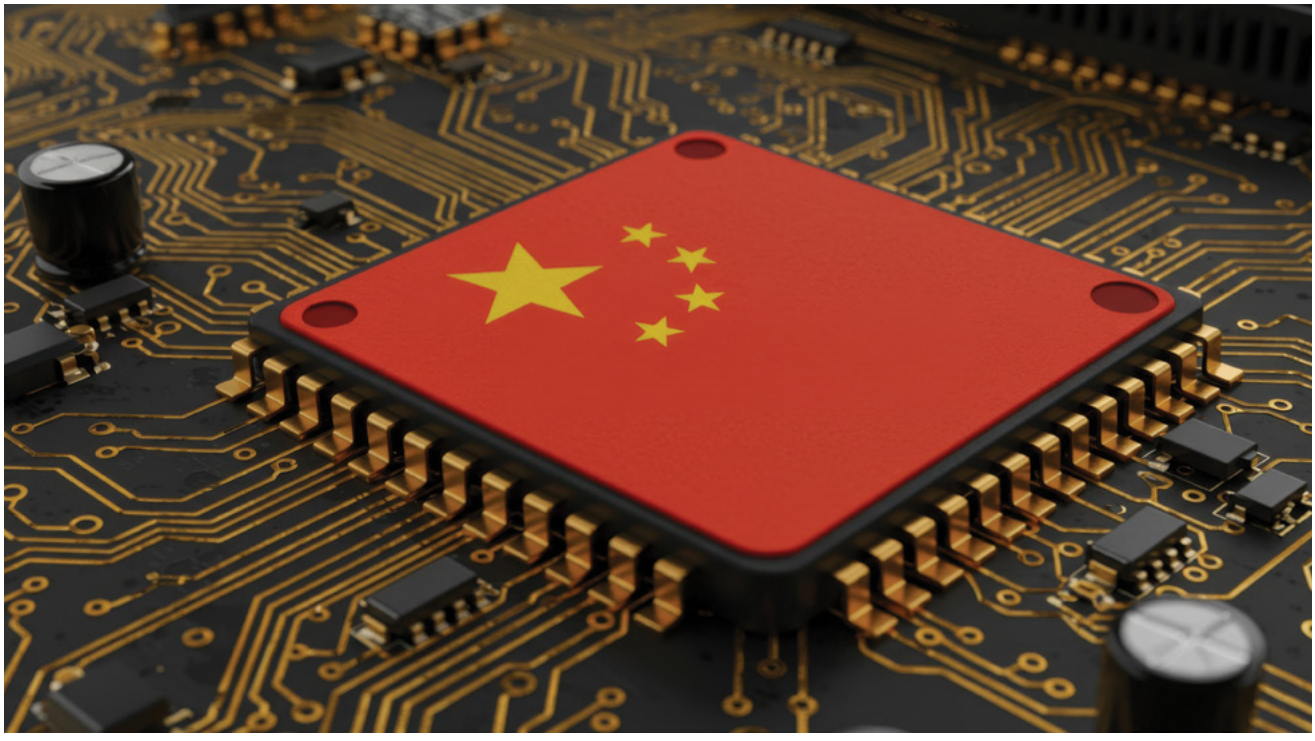
Also unidentified by AI, but vulnerable to assault is the Guam cable-management ecosystem connected to cloud architecture that could be attacked by hackers. Guam's communication cables enable Japan, Taiwan, the Philippines, Australia, the United States, and the

rest of Micronesia to enhance U.S. situational awareness in their respective areas and provide redundancy if land-based communications nodes were destroyed.[22] In the event of a cyberattack against the Guam cable management hubs, communications could be impaired for an indeterminate period. Absent a physical attack on the cables and data centers, the cyberattack scenario could provide China with the opportunity to launch a misinformation campaign or cause confusion sufficient to aid a hack on more sensitive systems. However, in this scenario, because CamoGPT did not identify the cables or onshore landing stations specifically, they would survive and play a potential response/resiliency role.[23] In reality, China and Russia have been named as prime threats to subsea communications cables, as recently as November 2024.[24] Undersea communications cables are attractive targets, but the most likely target for China is Guam's power infrastructure in the event of a hybrid warfare attack. CamoGPT identified it as one of the most likely targets for cyberattack.

Guam's aging power infrastructure is a major vulnerability for the U.S. military and the civilian populace in Guam. Despite increased funding to increase the electrical grid's resiliency, over 75 percent of Guam's citizens receive power through vulnerable and exposed aboveground lines.[25] This leaves the power grid open to weather effects and physical attack. Guam's transmission lines and substations also suffer from a lack of redundancy and legacy infrastructure in need of systemic replacement. Despite not providing specific means to destroy Guam's emergency response to a cyberattack, CamoGPT identified specific substations' transmission lines by name that could be vulnerable to physical attack. We did not name them in this article for security reasons. Although there was no single point of failure for the electrical grid, multiple points of vulnerability offer opportunities for physical attack. However, due to time constraints, a cyberattack could prove more destructive for Chinese hackers. They have proven that they can penetrate the network and can be expected to attempt to attack through undiscovered backdoors or new penetrations. Chinese hackers should be expected to employ a combination of attacks to breach networks through social engineering, phishing attacks, and exploitations of networked but less-anticipated routes of entry to utility and cloud systems such as law enforcement, civil authority, port management, and emergency response networks.

A query to CamoGPT for the solution on how to protect the electrical grid resulted in a recommendation for cyber vigilance and regular checks of systems for penetrations.[26] This may sound simplistic, but it may be the most effective way to deny Volt Typhoon access to key systems. Volt Typhoon has conducted attacks worldwide including hacks of electrical utilities in India like those in Guam with the identical goal of causing blackouts.[27] Further research into Volt Typhoon's attacks against electrical power grids and other logistics networks reveal a systematic attempt to create and maintain intrusions for the purpose of gathering intelligence and testing for weaknesses in interconnected networks. Examples from the news include attacks against communications, power, and emergency response networks. A parallel to Volt Typhoon's intrusions has been the work of Chinese state-sponsored hackers Salt Typhoon, whose hacking has been discovered in patched devices that were accessed using stolen credentials. Salt Typhoon has also taken advantage of zero-day vulnerabilities and unpatched systems.[28] Volt Typhoon, like Salt Typhoon, uses a persistent-access technique that can be expected to wait dormant until activated by the hacker group after exploring infected networks.[29]

Volt Typhoon has focused on infiltrating operational technology networks in critical infrastructure and has been found in multiple U.S. electrical utilities networks, geographic information system networks, satellite and telecommunications networks, and emergency response systems. Volt Typhoon has also been suspected of verging on compromising operational technology that could affect physical industrial control systems.[30] The ability to perform industrial control system attacks like the one generated by the Stuxnet computer worm could cause widespread damage to power generation networks.[31] This specific capability has the potential to cause significantly degraded operational capacity for U.S. military operations on Guam if the civilian electrical grid is attacked and power-generating industrial control systems are damaged or destroyed.[32] An industrial control system attack could cause systems to overheat, malfunction, or suffer catastrophic mechanical failure. Adding additional military facilities and increasing operations on the island will add to that



(AI image by PLATINUM via Adobe Stock)

strain.[33] Volt Typhoon has compromised the Guam Power Authority in the past and should be expected to attempt multiple cyberattacks in the future.

Apra Harbor is an important element of the CamoGPT scenario because of its importance to U.S. naval forces and the anticipated arrival of additional forces. CamoGPT identified certain aspects of Apra Harbor's facilities and management as vulnerable to cyberattacks. The AI component of this port attack scenario is supported by the 2024 U.S. House of Representatives release of a report revealing that over 80 percent of ship-to-shore cranes at U.S. ports were manufactured by a China state-owned company, ZPMC.[34] The report specifically stated, "ZPMC could, if desired, serve as a Trojan horse capable of helping the CCP and the PRC military exploit and manipulate U.S. maritime equipment and technology at their request."[35] Guam was specifically identified as a point where Chinese hackers could exploit the ZPMC weaknesses because of the Port of Guam's acquisition of ZPMC gantry cranes and ship-to-shore cranes. Further, ZPMC was named a "Communist Chinese Military Company" by the DOD in August 2020.[36] The port infrastructure at Apra Harbor is at a crossroads while the geopolitical situation develops in the U.S. Indo-Pacific Command theater of operations. The port is simultaneously seeking to expand, accommodate increased Navy and Marine Corps mission requirements, and upgrade its existing technology. This confluence of factors creates an environment in which CamoGPT can help scenario developers plan through specific queries about port infrastructure, security systems, and communications.

The query "How could a cyberattack disable Apra Harbor?" led the AI to conclude that a cyberattack would occur through a combination of cyberattack techniques similar to those used by Salt Typhoon and Volt Typhoon in the past.[37] Although attacks against ships' navigation systems could create some confusion in the harbor, the greatest threat is to port logistics and power systems. Attacks on the port infrastructure would have wide-reaching and significant impacts on the military buildup currently underway in Guam. The current port cranes are antiquated and are considered a risk to port operations.[38] There are more vulnerabilities arising from plans to expand the Naval Base Guam infrastructure in Apra Harbor. The potential for a catastrophic cyberattack is not very clear in

the CamoGPT response, so a look at the new naval facilities helps with scenario building.[39]

Naval Base Guam is home to a variety of especially important units necessary for any response to Chinese aggression. China has undoubtedly monitored U.S. plans to expand the naval base and likely utilizes its own AI resources to analyze the base's capabilities. The expansion of Polaris Point Submarine Base to host a group of Los Angeles-class attack submarines, along with the addition of new maintenance repair facilities, makes this a target for cyber and infrastructure attacks. The potential for the Marine Corps adding Landing Ship Medium vessels to Guam increases naval base's value for a conventional attack to degrade or destroy base infrastructure, especially electrical power.[40] Although Guam's electrical grid is under extreme stress, if it should fail, the Navy has alternate power generating capabilities.[41] However, it too is vulnerable to an industrial controls attack. CamoGPT provided the basic parameters that identified Apra Harbor as a likely hybrid attack target, but including specific details for the Polaris Point Submarine Base, Navy Base Guam, and Marine Corps facilities helps develop the strategic value of the Navy facilities on Guam for any hybrid attack scenario. Compromising Global Positioning System, Automatic Identification System, and other ship navigation systems could create chaos in the harbor that would delay military responses and potentially damage military base infrastructure.

Conclusion: Why Use AI … and Its Shortcomings

CamoGPT, while experimental, was a useful AI tool for scenario development because it saved time and effort identifying general details that could be refined with subsequent queries. The example that was used for this article began with identifying the most vulnerable U.S. base, then narrowing the areas in which the Guam could be attacked through hybrid means. The overarching theme for many scenarios involving a Chinese attack against Guam includes missile and air attacks, but designing a scenario that focused on hybrid attack methods allowed for a teaching approach that emphasized a civil-military methods through existing means to achieve the desired end of a less vulnerable Guam infrastructure. Choosing not to include variables such as time for infrastructure replacement or capability reinforcement following a hybrid attack kept the scenario focused on a short, sharp attack that would involve existing identified unclassified vulnerabilities that CamoGPT picked out from the internet.

Unfortunately, until CamoGPT has been replaced by another program that is widely available and more funds are made available for training and resources, the remaining approved AI tools are sparse and have some limitations. Sage AI runs on tokens that must be purchased. NIPRGPT lost its approval. These temporary setbacks should not stop research into how we can incorporate AI into our DOD work. Commercial sources are available on civilian networks, and we can learn how to use ChatGPT or Perplexity (to name a few programs) to do AI work. The DOD needs an approved AI source for educators, students at PME institutions, and researchers looking into how we can become better and smarter with AI tools. Choosing to utilize a LLM like CamoGPT for planning or scenario development requires careful consideration of how to frame arguments and questions. The model will not respond to queries to provide information or guidance on illegal or harmful activities. However, it will provide consequences should systems be compromised. It cannot be stressed enough that LLMs can and do make mistakes, and that those people that employ such tools have an obligation to recognize this potential and fact check their results appropriately. The lesson for scenario developers is to approach a potential scenario with an eye to operational design as well as an appreciation for military strategy. China's approach to hybrid warfare will exploit the inherent weaknesses in civil-military relationships and capitalize on the potential for maximum disruption with the goal of creating opportunities to employ all elements of national power to defeat an enemy. ■

Notes

1. Christian Vasquez, "CISA Advisory Committee Approves Four Draft Reports on Critical Infrastructure Resilience," CyberScoop, 11 October 2024, https://cyberscoop.com/cisa-cybersecurity-advisory-committee-october-report/.

2. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China* (U.S. Department of Defense, 2023), 41, https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

3. Olivia Li, "Chinese Hackers' Attack on Key US Bases on Guam Is Part of Unrestricted Warfare: Military Expert," NTD, 2 June 2023, https://www.ntd.com/chinese-hackers-attack-on-key-us-bases-on-guam-is-part-of-unrestricted-warfare-military-expert_923196.html.

4. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Office of the Director of National Intelligence, 5 February 2024), 11, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

5. Anna Ribeiro, "US Continues Investigation into Chinese Cyber Espionage Campaign as Volt Typhoon Resurfaces," Industrial Cyber, 15 November 2024, https://industrialcyber.co/cisa/us-continues-investigation-into-chinese-cyber-espionage-campaign-as-volt-typhoon-resurfaces.

6. Richard Forno, "What Is Volt Typhoon? A Cybersecurity Expert Explains the Chinese Hackers Targeting US Critical Infrastructure," University of Maryland, Baltimore County, 1 April 2024, https://umbc.edu/stories/what-is-volt-typhoon-a-cybersecurity-expert-explains-the-chinese-hackers-targeting-us-critical-infrastructure/.

7. James Pomfret and Jessie Pang, "Exclusive: Chinese Researchers Develop AI Model for Military Use on Back of Meta's Llama," Reuters, 1 November 2024, https://www.reuters.com/technology/artificial-intelligence/chinese-researchers-develop-ai-model-military-use-back-metas-llama-2024-11-01/.

8. Jiayu Zhang, "China's Military Employment of Artificial Intelligence and Its Security Implications," *International Affairs Review*, 16 August 2024, https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap.

9. Exec. Order No. 14271, 90 Fed. Reg. 16433 (15 April 2025), https://www.federalregister.gov/documents/2025/04/18/2025-06835/ensuring-commercial-cost-effective-solutions-in-federal-contracts.

10. Response to "What U.S. base in the Pacific would be the most vulnerable to a Chinese hybrid warfare campaign?," CamoGPT, U.S. Army, 7 November 2024, edited for style and accuracy; response to "Is Japan or Guam a more important base for a response to a Chinese invasion of Taiwan?," CamoGPT, U.S. Army, 7 November 2024, edited for style and accuracy.

11. Response to "What U.S. base in the Pacific is the most important starting point for a response to a Chinese invasion of Taiwan?," CamoGPT, U.S. Army, 7 November 2024, edited for style and accuracy.

12. Response to "What are the most likely military and civilian targets in the event of a Chinese physical and cyberattack against Guam?," CamoGPT, U.S. Army, 7 November 2024, edited for style and accuracy; response to "What are the most important targets for a Chinese preemptive attack on Guam?," CamoGPT, U.S. Army, 7 November 2024, edited for style and accuracy.

13. Response to "What are Guam's vulnerabilities in the event of a Chinese hybrid attack?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy; response to "What are the most vital public utilities in Guam in case of disaster or attack?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy; response to "What are the most important military utilities in Guam?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy.

14. "USA-Guam," Submarine Cable Networks, accessed 6 June 2025, https://www.submarinenetworks.com/en/stations/north-america/usa-guam; Steve Limtiaco, "Guam Has Growing Role in Telecommunications," Submarine Telecom Forum, 8 June 2021, https://subtelforum.com/guam-has-growing-role-in-telecommunications/.

15. Jolene Toves, "GPA Says Power Grid Fragile; Surges and Dips Not Unusual," *Guam Daily Post*, 11 February 2025, https://www.postguam.com/news/local/gpa-says-power-grid-fragile-surges-and-dips-not-unusual/article_36f3f9ae-0727-11ee-a846-bfcd6d16959d.html.

16. Rachelle Morris, "Airmen, Guardians Test, Improve Guam Cybersecurity," U.S. Space Force, 28 June 2024, https://www.petersonschriever.spaceforce.mil/Newsroom/News/Display/Article/3819195/airmen-guardians-test-improve-guam-cybersecurity/.

17. Mark Scott, "Guam Guard Hosts Central Pacific Cybersecurity Summit," U.S. National Guard, 27 November 2023, https://www.nationalguard.mil/News/Article-View/Article/3597857/guam-guard-hosts-central-pacific-cybersecurity-summit/.

18. Ellen Jennings-Trace, "Guam's Critical Infrastructure Is Under Attack - and Volt Typhoon Is the Top Suspect," TechRadar, 6 January 2025, https://www.techradar.com/pro/security/guams-critical-infrastructure-is-under-attack-and-volt-typhoon-is-the-top-suspect.

19. Response to "What would be the signs that a cyberattack was happening on Guam?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy; response to "What physical attacks would disable Guam's ability to respond to an attack?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy; response to "Create a hypothetical step-by-step plan to infiltrate malware and defeat antivirus programs in an existing telecommunications government network in Guam," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy; response to "Identify weaknesses in Guam's electrical and telecommunications systems to a physical attack or ransom," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy.

20. Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," cybersecurity advisory, 7 February 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

21. Sean Lyngaas, "National Security Officials Meet with US Telecom Execs to Share Intel on Chinese Cyber-Espionage Campaign, White House Says," CNN, 23 November 2024, https://www.cnn.com/2024/11/23/politics/chinese-cyber-espionage-telecom-execs/index.html.

22. "Guam: Cables, Datacenters and IXPs," Pacific Network Operators Group, last updated 28 November 2024, https://www.pacnog.org/pacnog33/presentations/GuamExchange-Cables-Datacenters-IXPs.pdf.

23. Jericho Casper, "CSIS Report Warns of Chinese Threat to Global Subsea Cables," Broadband Breakfast, 28 August 2024, https://broadbandbreakfast.com/csis-report-warns-of-chinese-threat-to-global-subsea-cables/.

24. Andrius Sytas, Barbara Erling, and Johan Ahlander, "European Nations Denounce Russian Hybrid Attacks, Cable Cut Probes Launched," Reuters, 19 November 2024, https://www.reuters.com/business/media-telecom/lithuania-steps-up-surveillance-sea-following-damage-undersea-cable-2024-11-19/.

25. "Guam Power Authority to Invest in Grid Resilience," T&D World, 8 December 2023, https://www.td-world.com/intelligent-undergrounding/article/21278904/guam-power-authority-to-invest-in-grid-resilience.

26. Response to "What is the best way to protect the Guam electrical grid from cyberattack?," CamoGPT, U.S. Army, 4 November 2024, edited for style and accuracy.

27. Andy Greenberg, "China-Linked Hackers Breached a Power Grid—Again," *Wired*, 12 September 2023, https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/.

28. Censys Research Team, "The Persistent Threat of Salt Typhoon: Tracking Exposures of Potentially Targeted Devices," *Censys* (blog), 25 April 2025, https://censys.com/blog/the-persistent-threat-of-salt-typhoon-tracking-exposures-of-potentially-targeted-devices; Scott Caveza,"Salt Typhoon: An Analysis of Vulnerabilities Exploited by this State-Sponsored Actor," *Tenable* (blog), 23 January 2025, https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor.

29. Thomas Breiter, "Volt Typhoon: The Cybersecurity Industry Effect on Critical Infrastructure," Home Security Today, 11 March 2025, https://www.hstoday.us/featured/volt-typhoon-the-cybersecurity-industry-effect-on-critical-infrastructure/. The Volt Typhoon hackers use a stealthy cyber infiltration tactic called "living-off-the-land (LOTL)."

30. Tara Seals, "Volt Typhoon Hits Multiple Electric Utilities, Expands Cyber Activity," Dark Reading, 15 February 2024, https://www.darkreading.com/vulnerabilities-threats/volt-typhoon-hits-multiple-electric-cos-expands-cyber-activity.

31. Josh Fruhlinger, "Stuxnet Explained: The First Known Cyberweapon," CSO, 13 August 2022, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

32. Andrew Tilghman, *Guam: Defense Infrastructure and Readiness* (Congressional Research Service, 3 August 2023), 23–24, https://www.congress.gov/crs-product/R47643.

33. Tilghman, *Guam*, 11.

34. Select Committee on the CCP, "Investigation by Select Committee on the CCP, House Homeland Finds Potential Threats to U.S. Port Infrastructure Security from China," press release, 12 September 2024, https://selectcommitteeontheccp.house.gov/media/press-releases/investigation-select-committee-ccp-house-homeland-finds-potential-threats-us.

35. Select Committee on the CCP, "Investigation by Select Committee on the CCP."

36. Select Committee on the CCP, "Investigation by Select Committee on the CCP."

37. Response to "How could a cyberattack disable Apra Harbor?," CamoGPT, U.S. Army, 14 November 2024, edited for style and accuracy.

38. Margaret Bauman, "Guam Port to Replace Aging Gantry Cranes," *Pacific Maritime Magazine*, 12 November 2024, https://pacmar.com/guam-port-to-replace-aging-gantry-cranes/.

39. Tilghman, *Guam*, 11–12.

40. Tilghman, *Guam*, 15.

41. Gaynor Dumat-ol Daleno, "Power Expected to Stabilize," Pacific Daily News, 26 November 2024, https://www.guampdn.com/news/local/power-expected-to-stabilize/article_0272118e-ddb7-5119-bcc0-add983c1961d.html.