



Online ISSN: 3006-5879 Print ISSN: 3006-5860

DOI: <https://doi.org/10.63468/jpsa.4.2.53>

Vol. 4 No. 2 (2026)

<https://journalpsa.com.pk/index.php/JPSA/about>



Recognized by: Higher Education Commission (HEC), Government of Pakistan

Digital Deterrence and the Militarization of Artificial Intelligence: Sino-US Grey Zone Competition in the South China Sea

Aima Ishaq

M.Phil Scholar Department of International Relations University of Sargodha

Dr. Ashfaq Ahmed *

Chairman Department of International Relations University of Sargodha

ashfaq.hameed@uos.edu.pk

Dr. Adil Iqbal

Assistant Professor, Department of International Business & Marketing, NUST Business School (NBS), National University of Sciences and Technology (NUST), Islamabad, Pakistan

* Corresponding Author

ABSTRACT

The United States (US) and China's growing strategic rivalry in the South China Sea has shifted away from traditional military posturing and toward technologically advanced grey zone conflict. This article looks at how the emergence of digital deterrence, and the militarization of artificial intelligence (AI) are changing the dynamics of maritime security in the area. It contends that the South China Sea has become a digitally contested battlefield where strategic influence is used below the level of open warfare due to digitally enabled surveillance systems, self-sufficient maritime platforms, satellite reconnaissance, cyber capability, and intelligent command-and-control infrastructures. To attain information dominance, improve maritime domain awareness, and discourage adversary acts through persistent tracking and predictive analytics, the paper examines how both China and the US use AI-driven Intelligence, surveillance and Reconnaissance (ISR) systems. U.S. developments in AI-enabled naval reconnaissance, unmanned defense systems, and related digital security architectures are compared with China's integration of intelligent warfare concepts, AI-powered radar systems, maritime sensor networks, and unmanned surveillance platforms. The article goes on to say that digital deterrence is different from traditional deterrence in that it depends more on data

dominance, algorithmic prediction, cyber resilience, and real-time visibility than it does on kinetic reprisal. The paper shows that AI is not just a technological tool but an enabler of strategic growth that is redefining power projection, escalation management, and strategic security in maritime grey zone conflicts through the theoretical lenses of Neorealism, Cross-Domain Deterrence, and Technological Constructivism. The study concludes that although AI-enhanced deterrence may lessen the possibility of direct military conflict, it also raises the dangers of unintentional escalation in the South China Sea, accelerates security issues, and intensifies surveillance competition.

Keywords: Artificial Intelligence, Sino-US Competition, South China Sea, Grey Zone Warfare, Maritime Surveillance, Cross-Domain Deterrence, Strategic Stability, AI Militarization

INTRODUCTION

The changing dynamics of the strategic rivalry between the United States and China are more clearly seen in the "grey zone," where influence, signaling, and coercion take place outside of regular diplomacy but below the line of open conflict. In contrast to traditional military conflicts, grey zone competition uses non-kinetic weapons and ambiguity to tip the scales without starting a frontal conflict. Artificial intelligence (AI) has become a game-changing facilitator in this regard, changing how the US and China manage information, project strategic behavior, and carry out surveillance. AI's incorporation into marine monitoring, cyber operations, and surveillance systems exemplifies a new stage of competitive interaction in which states combine state-of-the-art breakthroughs with conventional security measures.

China is using AI-powered tools to enhance situational awareness, speed up decision-making, and project superiority in disputed maritime areas as part of its aggressive stance in the Taiwan Strait and its expanded goals in the South China Sea, among other places. In keeping with a larger battle for technological and strategic dominance, the US simultaneously aims to offset China's technology advancements with its own AI-enabled defense programs, naval surveillance systems, and cyber counteroperations. The line between peace and conflict is blurred in cyberspace, as AI-enhanced cyber technologies allow for complex signaling, automated intrusions, and digital espionage. This paper's goal is to examine the operationalization of AI-enabled systems in the context of the US-China grey zone competition. This academic study illustrates the changing trends of AI-powered strategic behavior through case studies of three crucial domains: AI-enabled monitoring of the Taiwan Strait, artificial intelligence-driven surveillance in the South China Sea, and AI as a weapon in cyber operations and digital signaling. By looking at these instances, the analysis highlights how new technologies alter the deterrence calculation in the cyber and maritime sectors while also strengthening state power. The paper concludes by arguing that the incorporation of AI within grey zone competition raises the dangers of escalation in U.S.-China relations by complicating classic deterrence theory through boosting the

speed, ambiguity, and size of strategic interactions.

Sino- US Strategic Competition in Grey Zone

I. CASE STUDY: Use of AI for Surveillance of South China Sea

The socio-economic, political, and security significance of the South China Sea makes it as one of the most strategically important maritime areas in the world. Nearly one-third of the world's trade, valued at over \$3.4 trillion in products in 2023, goes through its crucial maritime lanes (Council on Foreign Relations [CFR], 2023). Competition is further fueled by the region's estimated 190 trillion cubic feet of natural gas reserves and 11 billion barrels of oil (U.S. Energy Information Administration [EIA], 2024). The 2016 Permanent Court of Arbitration decision in favor of the country of the Philippines under the United Nations Convention on the Law of the Sea (UNCLOS) invalidated China's claim of sovereignty over nearly 90% of the South China Sea through the "Nine-Dash Line." But through naval patrols, the militarization of manmade islands, and recently, particularly, AI-enhanced surveillance systems, Beijing has persisted in establishing control. The defense of allied national security and freedom of navigation continues to be essential components of US Indo-Pacific policy (Agnihotri et al., 2023). In addition to bolstering information, surveillance, and reconnaissance (ISR) systems with artificial intelligence (AI), Washington carries out Freedom of Navigation Operations (FONOPs) to counter China's exaggerated claims. As a result, the South China Sea serves as both a geographical hot spot and a test site for AI-driven grey zone tactics that gradually tip the scales without resorting to conflict.

AI-Powered Surveillance Capabilities carried out by China

China's use of AI for maritime security in the South China Sea has advanced quickly. The use of AI in conjunction with images from satellites, unmanned aerial vehicles (UAVs), and submerged acoustic sensors to establish a near-constant monitoring system throughout disputed waters is at the heart of Beijing's strategy. Using machine vision and big-data analytics, the PLA Navy and the China Coast Guard use AI-enhanced systems to recognize, categorize, and monitor vessels, both military and civilian. For instance, to track marine activity in real time, China's "Blue Ocean Information Network" combines satellites, drones, and AI-powered ocean buoys. Beijing can swiftly identify American or ally warships thanks to AI algorithms that analyse vast volumes of sensor and video data to find anomalies. Like this, AI-powered drones that can recognize images, like Wing Loong II and CH-5 UAVs, carry out continuous surveillance missions. In a direct challenge to American dominance in the underwater world, China is additionally using AI-enabled submerged drones that survey the seabed and monitor submarine activity.

The integration of commercial technologies such as facial recognition, port surveillance systems, and satellite firms like BeiDou into national security initiatives is guaranteed by China's civilian-military fusion policy. AI-powered cameras and sensors improve situational awareness in harbors and artificial islands, enabling Beijing to regulate maritime commercial activity and keep an eye on foreign vessels (Allen, 2022). These developments provide China a competitive edge in the grey area

since they enable it to progressively assert its interests without starting a full-scale war.

US Countermeasures Powered by AI

The US has made significant investments in AI-enabled maritime domain awareness (MDA) in recognition of China's increasing technological dominance. To establish AI-powered shared surveillance systems throughout the South China Sea, Washington has teamed up with allies including Japan, Australia, and the Philippines. AI is used in programs like the Indo-Pacific Partnership for Maritime Domain Awareness (IPMDA), which was introduced in 2022 and provides near-real-time vessel tracking by processing satellite data from both military and commercial sources (U.S. Department of Defence [DoD], 2023). The US military's ISR operations are also strengthened by AI. For instance, the Project Maven program, which was initially created for counterterrorism, has been modified for maritime surveillance by employing artificial intelligence (AI) to analyse drone and satellite images and automatically identify anomalous vessel patterns (Sayler, 2023). With the use of AI navigation and target identification systems, the U.S. Navy's Sea Hunter unmanned surface vessel can monitor surface ships and submarines on its own across extended distances (O'Rourke, 2024). Furthermore, to enhance situational awareness in disputed waters, DARPA's Ocean of Things initiative uses AI-powered submerged sensors to gather environment and vessel data (DARPA, 2022). The U.S. also incorporates regional counterparts into AI-enhanced information exchange through its alliance network. For example, increased ISR cooperation is part of the Philippines' recent agreement to increase U.S. base access in 2023. China's hegemony in the grey area is being challenged by Australia's drone patrol initiatives and Japan's AI-based satellite monitoring, which both add to an AI-enabled coalition surveillance system.

Strategic Implications

The deterrence equation between China and the US is altered by the deployment of AI reconnaissance in the South China Sea. In the murky area, AI also improves strategic signaling. For instance, Beijing conveys capacity and resolve without resorting to open warfare by showcasing its real-time tracking capabilities of U.S. vessels. Washington, on the other hand, is sending a counter-message of collective disagreement with unilateral Chinese claims using AI-enabled global monitoring. AI thus serves as a tool for coercion as well as deterrence, escalating the psychological aspects of the competition.

Grey Zone Dimensions

An example of the use of AI in a grey area is the South China Sea. China deliberately avoids thresholds that would lead to war by using gradual and ambiguous measures, such as tracking American ships, sending coast guard ships that are monitored by AI, and creating artificial islands. By automating detection, combining surveillance with military preparation, and giving Beijing deniability ("we are only monitoring our territory"), AI increases the effectiveness of these operations. In response, the US launches AI-powered FONOPs that fight China's encroaching expansionism while simultaneously upholding international law. By lowering

expenses and expanding operational reach, AI enables constant presence without face-to-face conflict.

Prospects for the Future

In the future, AI is probably going to make the South China Sea's grey zone competition more intense. While the U.S. stresses AI-integrated partnerships to preserve collective deterrence, China is moving towards completely autonomous swarms of drones and underwater vehicles to maintain dominance. Algorithmic escalation—where decisions are based on machine outputs rather than intentional diplomacy—is a risk that increases as both parties embrace increasingly autonomous systems. In the end, the South China Sea is a microcosm of the larger Sino-American rivalry, which is a conflict for both land and the capacity to incorporate new technologies into strategic actions. (Min, Zhao, Bu, Ding, & Wagner, 2023).

Case II: AI for Taiwan Strait Surveillance

In the current Sino-American strategic rivalry, the Taiwan Strait, a slender 180-kilometer strait that divides Taiwan from mainland China, has emerged as one of the most delicate flashpoints. The strait serves as a vital marine route for international trade and energy flows in addition to being a geopolitical fault line. Taiwan is a "core interest" for China, and the Chinese Communist Party (CCP) continues to view its reunification as a top priority, supported by Beijing's military modernization and "civil-military fusion" policies. To preserve the rules-based global system and the United States' reputation in the Indo-Pacific, Taiwan's security must be preserved. Formalizing the "Six Assurances" could bring much-needed stability during tensions between the United States and Taiwan, according to Rigger (2025).

China's AI-Powered Taiwan Strait Surveillance

To keep an eye on Taiwan and discourage American intervention, China has made significant investments in AI-driven surveillance, reconnaissance, and intelligence gathering (ISR) capabilities. Beijing tracks naval operations across the strait using autonomous drones, undersea acoustic sensors, and AI-powered satellite pictures. The PLA's pursuit of "human-machine hybrid intelligence" in the fields of biotech, brain science, and artificial intelligence as demonstrated by Kania (2020) that the People's Liberation Army (PLA) can anticipate possible U.S. or Taiwanese maneuvers because to these technologies' integration with artificial intelligence algorithms that analyses enormous volumes of real-time data. The distinction between normal monitoring and military intimidation has been blurred, for example, by the deployment of AI-enabled drones throughout Taiwan's Air Defense Identification Zone (ADIZ). According to reports, China's "Great Underwater Wall" project, which was once intended for monitoring the South China Sea, has being extended towards the Taiwan Strait. It uses acoustic sensor networks and artificial intelligence (AI) to identify submarine operations.

The PLA Navy's advancements in undersea combat and surveillance capabilities are highlighted in the CMSI (2023) conference report. AI is also used by China in its information warfare against Taiwan. Digital propaganda efforts are employed to monitor opposition in Taiwan and sway its political discourse using AI-

enabled facial recognition, big data analytics, and natural language processing. The Thomson Foundation (2024) claims that during Taiwan's 2024 election, disinformation efforts powered by AI profoundly influenced the information landscape. By influencing views and weakening Taiwan's resistance, such actions, albeit not being explicitly kinetic, support Beijing's strategic signaling in the grey area. China's concept of "intelligentized warfare," in which AI serves as both a tactical enabler and a tool for political coercion, is highlighted by the incorporation of AI beyond conventional and unconventional domains.

AI Countermeasures by the US and Allies

In response, the US has bolstered its own AI-driven ISR capacities in the Taiwan Strait after realizing the strategic ramifications of PLA spying enabled by AI. To keep an eye on Chinese military action in real time, the U.S. Indo-Pacific Command (INDOPACOM) is depending more on AI-enabled satellite analytics, modelling for prediction, and unmanned aerial systems. U.S. forces can track Chinese drones, vessels, and aircraft close to the strait because to programs like Project Maven, which uses machine learning to analyse video imagery, and have been modified for Indo-Pacific navy surveillance (Department of Defense, 2023). Additionally, through the Quad and AUKUS agreements, Washington has increased intelligence cooperation with regional allies like Australia and Japan. To establish a shared operational image of the Taiwan Strait, these partnerships entail incorporating AI-powered maritime domain awareness (MDA) technologies, which employ sensor fusion and machine learning (Hanson, Grissom, & Mouton, 2024). To counter China's increasing surveillance dominance, Taiwan has made investments in AI-based early warning systems, cyber defense platforms, and unmanned aerial vehicles (UAVs), frequently with technology assistance from the United States (Altman & Porter, 2023). AI helps the U.S. and its allies to better deterrent posture, maintain escalation oversight in the grey zone, and discover anomalies more quickly by improving predictive analytics and decreasing need on human operators.

Applications of AI and Grey Zone Dynamics

Grey zone rivalry is best shown by the Taiwan Strait, where gradual, ambiguous, and non-kinetic strategies are used to exert coercion and deterrence. China regularly launches "drone swarms" and simulates invasion drills close to Taiwan's waters, purposefully setting the scales below the point of conflict. By facilitating adaptive operations, increasing the physiological pressure on Taiwan, and optimizing decision-making speed, AI strengthens these strategies (Huang & Tsai, 2022). Meanwhile, American deterrence tactics are made more difficult by AI-powered spying. China's AI-enabled ISR gives it an informational edge over the United States, which prioritizes freedom of navigation operations (FONOPs) and deterrence through presence. This enables Beijing to precisely anticipate and shadow U.S. maneuvers. The ambiguity that is essential to grey zone competitiveness is reinforced by this interaction, which produces a feedback cycle in which both parties increase the level of surveillance without going into open conflict.

Implications for Strategy and the Future

The use of AI in Taiwan Strait monitoring has significant effects on stability and deterrence. In the future, the Taiwan Strait AI battle is probably going to get fiercer. Deeper adoption of data science, machine learning, and autonomous systems into PLA operations is suggested by China's ambitions to attain "AI supremacy" by 2030. To offset Beijing's technological superiority, the United States is probably going to deepen its alliances with Taiwan and other allies in the region. The hazards of algorithmic error and quick escalation could pose the greatest threat to regional security in the Taiwan Strait as both sides use AI as a weapon for grey zone competitiveness.

Case III: Using AI as a Tool for Cyber Operations and Grey Zone Digital Signaling History of Cyberwarfare in Sino-American Relations

One of the most hotly fought areas of Sino-American strategic competition is the cyber domain, which serves as both a special area of grey zone warfare and an extension of conventional deterrence. Artificial intelligence (AI) is ideally suited to cyber conflict because, in contrast to conventional or nuclear threats, it feeds on ambiguity, covert signaling, and the difficulties of attribution. With AI acting as a multiplier of force that improves surveillance, incursion, defense, and signaling capabilities, both China and the United States acknowledge the importance of cyber power to national security. Mandiant (2022) says that by facilitating propaganda, cyber espionage, and the sabotage of vital infrastructure, cyber operations frequently support physical maneuvers in the Taiwan Strait and South China Sea. The distinction between peace and combat is further blurred by the application of AI in this field, which increases operations' speed, scope, and sophistication.

China's Cyber Capabilities Driven by AI

In line with its intelligentized warfare philosophy, which aims to integrate AI in both military and civilian spheres, China has made significant investments in AI-enhanced cyber capabilities. To break into American and allied networks, the Chinese People's Liberation Army (PLA) has created artificial intelligence (AI) tools for adaptive phishing campaigns, automated malware creation, and intrusion detection (Scharre & Kania, 2022). AI has been used more by state-affiliated hacking groups like APT10 and APT41 to automate reconnaissance, avoid detection, and quickly exploit weaknesses (Mandiant, 2023). Furthermore, China has used artificial intelligence (AI) as a weapon in disinformation efforts, distributing customized narratives in Taiwan and elsewhere using deep fake technology and natural language generation, eroding political unity and casting doubt on US commitments (Huang, 2024). As a kind of digital signaling to convey Beijing's will and technological prowess, these actions are not just tactical but also strategic. For instance, Council on Foreign Relations (2023) explains in detail that Chinese cyber operators allegedly used AI-augmented malware to probe Taiwanese government networks during heightened tensions around Taiwan in 2023, while also inundating social networking sites with AI-generated narratives of U.S. abandonment. These operations are designed to gradually change the balance of power while staying below the line of open combat.

U.S. Cyber Strategy Powered by AI

The United States has created a multifaceted response in recognition of the importance of AI in cyber deterrence. Intelligence-enhanced identification of anomalies, predictive analytics, and cyber defense automation are being funded by DARPA's AI Next initiative and the Department of Defense's Joint Artificial Intelligence Centre (JAIC) (DARPA, 2023). To facilitate what is known as "persistent engagement"—continuous operations intended to thwart adversary cyber assaults before they worsen—U.S. Cyber Command (CYBERCOM) has additionally implemented AI systems that can quickly attribute and counterattacks (Nakasone & Sulmeyer, 2020). Furthermore, under agreements like the Quad and AUKUS, the U.S. has stepped up its collaboration with allies like Japan, Australia, and Taiwan to develop AI-based cyber situational awareness technologies (Fischer, 2021). Washington sees AI as an offensive signaling weapon in addition to a protective shield. The United States intends to impose costs while carefully limiting escalation risks by launching limited, traceable cyber countermeasures against Chinese AI-assisted breaches. This relationship illustrates how Cold War deterrence is mirrored in AI-powered cyber competition, although with increased ambiguity, speed, and uncertainty.

AI's "Grey Zone" Aspects in Cyber Operations

Grey zone conflict, in which actors seek military and political goals below the line of kinetic warfare, is best exemplified by cyber operations. Because AI makes cyber incursions faster, more flexible, and more difficult to attribute, it exacerbates this issue. For example, Rid and Buchanan (2015) in their work explain, that how without firing a shot, an AI-generated deep fake video published during a crisis could cause confusion among U.S. or Taiwanese leadership. Similarly, autonomous malware that can change its own code might enter networks without obvious ties to the country of origin, giving China plausible deniability while yet exerting pressure. According to Beijing, military actions in the South China Sea and Taiwan Strait are complemented by AI-enhanced cyber measures, resulting in a multifaceted pressure campaign that undermines the confidence of U.S. deterrence. The difficulty for Washington is in adjusting its responses; a strong response could lead to escalation, while a modest response could encourage more violence in the grey area. AI-driven cyber operations are therefore strategic movements in the larger Sino-US competition rather than merely technical exchanges.

Implications for Escalation and Deterrence

Traditional deterrence reasoning is made much more difficult by the incorporation of AI onto cyber operations. First, because AI can automate vulnerability detection and overload defenses, it speeds up the offense-defense balance (Barrett et al., 2023). Second, it creates the possibility of unintentional escalation since disproportionate reaction may result from incorrect attribution or computational errors. Finally, AI-enabled signaling obscures intent since modest intrusions and misinformation operations could be seen as either regular espionage or acts leading up to a bigger battle. AI-enabled cyber capabilities provide China with

an affordable way to weaken American dominance in the Indo-Pacific without having to face the dangers of direct conflict. They provide the US a chance to improve cyber resiliency as well as a challenge in upholding credible deterrence. Crisis stability is becoming increasingly precarious due to the ambiguity surrounding AI-driven cyber transactions.

Prospects for the Future

The AI-powered cyberwarfare between the United States and China is probably going to get more intense in the future. The scope and velocity of grey zone techniques will increase as both nations incorporate machine learning and quantum computer technology into their cyber operations. Conflict thresholds may be redefined by new threats like AI-orchestrated botnets, autonomous cyberweapons, and sophisticated deep fake propaganda (Allison, 2024). The possibility of unintentional escalation by means of AI-enabled cyber operations remained considerable in the absence of established standards or arms control mechanisms.

CONCLUSION

To analyse how artificial intelligence is influencing Sino-U.S. deterrence dynamics in the grey zone, this chapter has looked at three important case studies: The South China Sea, the Taiwan Strait, and artificial intelligence-powered cyber operations. When taken as a whole, these examples show that AI is more than just supporting technology; rather, it is a revolutionary force that is changing the nature of strategic engagement in the Indo-Pacific. The results show that AI acts as a double-edged sword that alternately erodes stability and increases the credibility of deterrence by promoting both escalation and moderation.

REFERENCES

- Agnihotri, K. K., Chauhan, P., & Lahiri, D. (2023). Maritime security dynamics in the Indo-Pacific: Strategies and trends. National Maritime Foundation. https://www.researchgate.net/publication/376720408_Maritime_Security_Dynamics_in_the_Indo-Pacific_Strategies_and_Trends
- Allen, G. C., & Chan, T. (2017). Artificial intelligence and national security. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>
- Allison, G. T. (2017). *Destined for war: Can America and China escape Thucydides's trap?* Houghton Mifflin Harcourt.
- Altman, J., & Porter, P. (2023). The autonomous arsenal in defense of Taiwan: Technology, law, and policy of the Replicator initiative. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from <https://www.belfercenter.org/replicator-autonomous-weapons-taiwan>
- Barrett, C., Boyd, B., Bursztein, E., Carlini, N., Chen, B., Choi, J., Chowdhury, A. R., ... Yang, D. (2023). Identifying and mitigating the security risks of generative AI. *Foundations and Trends in Privacy and Security*, 6(1), 1–52.

- <https://doi.org/10.1561/33000000041>
- China Maritime Studies Institute (CMSI). (2023, May). Quick look summary: CMSI's 11–13 April 2023 conference on “Chinese undersea warfare: Development, capabilities, trends”. U.S. Naval War College. <https://www.andrewerickson.com/2023/05/quick-look-summary-cmsis-11-13-april-2023-conference-chinese-undersea-warfare-development-capabilities-trends>
- Council on Foreign Relations. (2023). *Territorial disputes in the South China Sea*. Retrieved from <https://www.cfr.org/> Council on Foreign Relations. (2023). *Territorial disputes in the South China Sea*. Retrieved from <https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea>.
- DARPA. (n.d.). *Ocean of Things*. Research Spotlights. Retrieved August 14, 2025. <https://imsehawaii.org/iuuf/ewExternalFiles/DARPA%20Ocean%20of%20Things.pdf>
- Fischer, J. (2021). AI politics and governance as an emergent security practice: Technological possibilities and political choices. *Swiss Political Science Review*. <https://doi.org/10.1111/spsr.12439>
- Hanson, R., Grissom, A. R., & Mouton, C. A. (2024). The future of Indo-Pacific information warfare: Challenges and prospects from the rise of AI. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA2205-1.html
- Huang, J., & Tsai, K. (2022). Securing authoritarian capitalism in the digital age: The political economy of surveillance in China. *The China Journal*, 88(1), 1–26. <https://doi.org/10.1086/720144>
- Mandiant. (2022). Mandiant Cyber Security Forecast 2023. Retrieved from <https://d110erj175o600.cloudfront.net/wp-content/uploads/2022/11/02144954/Mandiant-2023-Forecast-Report.pdf>
- Min, C., Zhao, Y., Bu, Y., Ding, Y., & Wagner, C. S. (2023). Has China caught up to the US in AI research? An exploration of mimetic isomorphism as a model for late industrializers. arXiv. <https://arxiv.org/abs/2307.10198>
- Nakasone, P. M., & Sulmeyer, M. (2020, August 25). How to compete in cyberspace. *Foreign Affairs*. Retrieved from <https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity>
- O'Rourke, R. (2024). China's naval modernization: Implications for U.S. Navy capabilities. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/RL/RL33153>
- Rid, T., & Buchanan, B. (2015). *Attributing cyber attacks*. Department of War Studies, King's College London. Retrieved from <https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf>
- Rigger, S. (2025, August 11). “The Six Assurances to Taiwan Act”: Status quo, or something new? Brookings Institution. Retrieved from [https://www.brookings.edu/articles/the-six-assurances-to-taiwan-act-status-](https://www.brookings.edu/articles/the-six-assurances-to-taiwan-act-status-quo-or-something-new/)

- [quo-or-something-new/](#).
- Sayler, K. (2023). Artificial intelligence and national security. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/R/R45178>
- Scharre, P., & Kania, E. B. (2022). Artificial intelligence and arms control. Center for a New American Security. Retrieved from https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AI-and-Arms-Control_FINAL.pdf
- Thomson Foundation. (2024). AI disinformation attacks target Taiwan's 2024 election. Thomson Foundation. https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf
- U.S. Department of Defense. (2023, November 2). DOD releases AI adoption strategy. U.S. Department of defense. <https://www.defense.gov/News/NewsStories/Article/Article/3578219/dod-releases-ai-adoption-strategy/>
- U.S. Energy Information Administration. (2024). South China Sea energy resources. U.S. EIA. <https://www.eia.gov/international/analysis/country/CHN>