

Fall 2025 - Marcellus Policy Analysis

Electronic Warfare and Crisis Stability in the US-China Gray-Zone Competition

By Selena Lin

EXECUTIVE SUMMARY

As the strategic competition between the United States and China intensifies, military interaction increasingly occurs below the threshold of armed conflict through persistent gray-zone activities. Among the most consequential of these activities is the use of electronic warfare (EW) to degrade sensing, navigation, and communication systems. This is particularly important as escalation between the two great powers, the United States, likely occur in the Indo-Pacific Region, where precise automated kill chains are necessary to maintain multi-domain awareness.

To demonstrate this, the report uses a scenario assessment of a gray-zone quarantine of Taiwan. The scenario follows phases of PLA use of ambiguous probing and attribution erosion, to enforce quarantine and sustained non-kinetic pressure on Taiwan. This demonstrates how EW can be integrated into an automated kill chain to determine the information environment and constrain adversary decision-making. The analysis shows that while adaptation and recovery may restore partial functionality, they do not necessarily restore pre-crisis conditions of deliberation and control. Instead, repeated cycles of disruption and response can narrow decision space and heighten escalation over time.

Selena Lin is a Master's student in International Affairs at the Georgia Institute of Technology. She previously interned with the Center for Strategic and International Studies' China Power Project, where she researched Chinese security policies and cross-Strait relations. In 2025, she was selected for Taiwan's Mosaic Fellowship, presenting policy and dialogue on societal and industrial resilience to Taiwan's Ministry of Foreign Affairs. She also participated in National Chengchi University's 2025 large-scale civilian wargame on a Taiwan contingency, contributing analysis on cyber defense, industry stability, and societal resilience.

The John Quincy Adams Society is a nonpartisan, independent national network of professionals and students focused on U.S. foreign policy, with a centering vision of restraint. The Society does not take specific policy positions and all views, positions, and conclusions expressed in this publication should be understood to be those of the author.

Based on this analysis, the report offers several policy recommendations aimed at preserving U.S. crisis stability under conditions of persistent interference. Current U.S. initiatives, such as Project Maven and the Replicator Initiative, emphasize rapid data integration and responsiveness in contested environments that risk accelerating uncertainty during gray-zone crises if not paired with escalation controls. The Department of Defense should require automated systems to demonstrate performance under degraded and ambiguous environments. U.S. operational policy should also formalize human-around-the-loop escalation controls by clearly specifying which functions may remain automated under contested conditions and which require human validation, particularly when automated outputs could cue cross-domain responses. Resilience planning should move beyond rapid recovery to assess sustained performance across multiple cycles of disruption and adaptation through joint exercises and wargames with Indo-Pacific partners. Finally, U.S. crisis management mechanisms should more directly address persistent electronic warfare by developing dialogue and confidence-building measures focused on managing ambiguity, clarifying interference affecting navigation, sensing, and command-and-control systems, and slowing escalation dynamics during prolonged gray-zone competition.

Introduction

Modern militaries increasingly turn to the speed and integration with which operations can process, interpret, and act upon information to target enemies. This process encompasses the “kill chain” at the most fundamentals level: find, fix, track, target, engage, assess (F2T2EA).¹ Like all revolutions in military affairs, kill chains do not represent the technological systems themselves. Rather, they are the organizational and technological frameworks within which military technologies operate that determine how quickly and reliably military force can be applied. For China, military modernization emphasizes kill-chain integration across domains. Throughout its modernization efforts, the People’s Liberation Army (PLA) has pursued system-level disruption by paralyzing an adversary’s command, control, and situational awareness without overt kinetic attacks.² These capabilities enable persistent, reversible electronic warfare that can be applied below the threshold of war under the guise of plausible deniability.

This alters crisis stability for the United States when interacting with China. Automated and semi-automated systems are designed to increase speed, integration, and

responsiveness. At the same time, these characteristics can compress decision cycles and magnify uncertainty when information becomes unreliable. Electronic warfare (EW) weaponizes plausible deniability by exploiting reversibility, difficult attribution, and natural and space weather disturbances. These effects expand the gray zone for coercive action while narrowing the margin for escalation control. The inability to manage crises in geopolitics creates destabilizing consequences. Even rational, risk-averse actors face incentives to act earlier when decision cycles are compressed and information is uncertain. For the United States, this creates a dilemma. Efforts to deter China by accelerating U.S. kill chains risk mirroring the very dynamics that undermine crisis stability.

The paper argues that China’s integration of automated kill chains and electronic warfare (EW) widens the gray zone for PLA activities and undermines crisis stability in the U.S.-China competition. The following analysis focuses on how repeated cycles of electronic interference and adaptation that degrade situational awareness can result in crisis instability even when all parties prefer de-escalation. A scenario assessment of automated kill chains and electronic warfare in the Taiwan Strait to demonstrate mechanisms that may emerge wherever automated kill chains operate under sustained electronic interference. A gray zone kill chain operates by shaping the information environment in which decisions are made, constraining adversary choices through sensing and persistent interference. Automation accelerates data fusion and tasking under conditions of degraded information, thereby compressing decision timelines.

The paper proceeds in four sections. The first section examines the literature on crisis stability, specifically how it is observed in gray-zone activities. The second section outlines the PLA doctrine surrounding electronic warfare and kill-chain integration across domains. The third section presents a PLA gray-zone quarantine of Taiwan to illustrate how the PLA doctrine is applied. The closing section discusses the policy implications for the United States and how to preserve crisis stability to avoid the inadvertent escalation in contested information environments.

Crisis Stability in the Gray-Zone

Crisis stability became a central concern during the Cold War, when nuclear proliferation forced great power competitors to manage crises without inadvertent escalation.³ In *Arms and Influence*, Thomas Schelling describes a crisis as stable when neither side believes

it must act first to avoid strategic disadvantage.⁴In the nuclear context, rather than being deterred and compelled through the use of force, nuclear weapons' coercive power lies in the context of not using them. While originally developed in the context of nuclear deterrence, crisis stability remains fundamental preserving control over escalation. However, this idea emerged in the context of unlimited war. Schelling's framework emphasizes cost-benefit calculations that determine whether actors believe they can afford to wait rather than strike first.⁵

In gray-zone competition, crises operate under different conditions. Coercive actions are deliberately calibrated to remain below the threshold of armed conflict and incremental rather than existential. As a result, deterrence stability is weakened not by an existential threat, but by persistent pressure that narrows decision space and forces earlier responses. Robert Powell (1989) offers a framework for understanding crisis stability under limited warfare. Powell argues that crisis stability depends on whether actors believe war has become inevitable rather than on the existence of fire-strike advantages.⁶ Thus, if actors believe restraint can avoid conflict, even favorable incentives to strike first do not produce instability.

In gray-zone competition, escalation is characterized by iterative interactions that shape beliefs rather than discrete escalatory decisions. Gray-zone strategies are deliberately designed to remain below the threshold to conventional military conflict, relying on incremental and ambiguous actions that accumulate advantage while avoiding overt escalation.⁷ Hal Brands characterizes gray-zone conflict as coercion that is "ambiguous and usually incremental," allowing revisionist states to pursue strategic gains while creating uncertainty over intent and attribution.⁸ This incrementalism creates the appearance that escalation can be carefully controlled. Gray-zone competition places sustained pressure on belief formation and crisis management. Thus, rather than clear intentions, iterative sub-threshold actions erode confidence over time. This is because escalation is inherently subjective, shaped by how actions are interpreted rather than intended. In gray-zone competition, this dynamic becomes purposeful to achieve escalation dominance, "the ability to escalate a conflict in ways that will be dangerously costly to the adversary while the adversary cannot do the same in return."⁹ As opposed to crossing clear red lines, escalation dominance is achieved by shaping beliefs over time, narrowing perceived response options without triggering overt conflict.

In these instances, direct kinetic conflicts are unfavorable and costly to the revisionist state. However, Robert Jervis argues, "To the extent that military balance is stable at the level of all nuclear war, it will become less stable at lower levels of violence."¹⁰ In the context of U.S.-China rivalry, this logic suggests that mutual confidence in strategic deterrence may inadvertently increase incentives for competitive behavior below the threshold of major war. Rather than reducing conflict, strategic stability can shift competition in gray-zone activities, where the perceived risks to of escalation risk more manageable.¹¹

The PLA Kill Chain Approach

PLA doctrine structures competition through the concepts of informationized and system destruction warfare, which emphasize information dominance and the disruption of an adversary's operational systems rather than decisive kinetic engagement.¹² According to the 2024 Department of Defense report on China's military and security developments, the PLA increasingly views modern conflict as one of information superiority and intelligentized disruption across domains.¹³ Within this framework, gray-zone actions are meant to remain below the threshold of armed conflict while undermining the adversary's ability to decide and coordinate effectively. Kill chains function as the underlying operational logic of these doctrines. While modern militaries all integrate a version of a kill chain, the PLA emphasizes the integration of sensors, command networks, and non-kinetic capabilities to compress decision cycles and enable rapid cross-domain effects. This increasingly automated integration is operationalized through the PLA's concept of integrated joint operations, which seeks to synchronize capabilities across land, air, maritime, space, and information domains under a unified command structure.¹⁴ Joint operations allow actions in one domain to generate immediate effects in another. Thus, the kill chain is transformed from a linear targeting process into a multi-domain web that enables rapid, coordinated responses. The PLA has relied heavily on persistent sensor architecture, ranging from space-based intelligence, surveillance, and reconnaissance (ISR) to maritime domain awareness systems. This webbed kill chain enables the PLA to maintain near-constant situational awareness in contested regions while simultaneously assessing adversaries' capabilities.

The PLA has demonstrated its commitment to expanding its EW capabilities. The Kuayue-2009 drills (also known as the Stride-2009 drills) were the first

known large demonstration of the PLA's information dominance and systems-destruction warfare through the integration of BeiDou GNSS and EW systems.¹⁵ Similar drills—like the Kuayue-2015, Joint Action 2014 and Joint Action 2015—utilized air-land integration and EW.¹⁶ Although the outcomes of these drills failed to demonstrate the mass information dominance the PLA intended, these events demonstrated the PLA's understanding of the operational value of EW. This is reflected in the restructured PLA Strategic Support Force (PLASSF), which now consists of the Cyberspace Force, Electronic Warfare Force, and Information Support Force.¹⁷ As noted by Xiaoke Qie, the People's Republic of China's 2025 military parade highlighted these forces as coordinated into a single information operations group, supporting the general operations of the PLA.¹⁸

In contested regions, such as the South China Sea and the Taiwan Strait, civilian, commercial, and military assets operate in close proximity. Thus, maintaining situational and domain awareness is difficult across maritime, air, and information domains. The PLA can employ methods such as jamming and spoofing to exemplify this ambiguity. Jamming prevents the reception of signals by propagating a high-power radio signal at the same or similar frequency as the target signal. This causes the receiver to either pick up the deceptive signal or experience an increased signal-to-noise ratio that drowns out the original signal.¹⁹ Spoofing can subtly manipulate data by transmitting signals similar to the target to deceive the receiver to “misinterpret fake signals as authentic ones.”²⁰ Because spoofing and jamming often do not produce clear kinetic damage or persistent effects, they impose higher geopolitical thresholds for response. Furthermore, the deployment of the PLA's EW capabilities is difficult to attribute, in part because EW effects can resemble environmental interference, equipment malfunction, or space-weather disturbances. Non-kinetic disruptions to satellite navigation, communications, or radar systems can be reversible and localized.

The PLA also has various EW-capable assets. The JN-Series EW systems contain mobile jammers that can also search and detect high-frequency radio frequencies.²¹ The Type 055 Destroyer has a H/LJG-346B Active Phased Radar System, which integrates large S- and X-band active sensors for onboard EW suite for jamming, spoofing and detection.²² The Type 052D Class (Luyang III) Destroyer includes the Type 726 EW suite, which features radar intercept receivers (726-1 and 726-5), a 726-2 direction finder, and the 726-3 radar jammer.²³ Although from a previous generation, the Type 052C Class (Luyang II) Destroyer

includes the NJR-6A EW electronic suite that is capable of sensing and jamming radio frequencies. Airborne jammers include the Y-8G/Y 9G designed for electronic attacks across a broad frequency range.²⁴ J. Michael Dahm noted that these aircraft will likely accompany bombers, such as the PLA Air Force (PLAAF) H-6 bombers, and support PLA Navy Air Forces (PLANAF).²⁵ The J-16D Electronic Warfare Aircraft's jamming pods at the wingtips offer a range of electronic attacks and support.²⁶

Commercial satellite imagery indicates that the PLA has constructed EW infrastructure in the South China Sea. This infrastructure includes high-frequency direction-finding (HFDF), mobile EW vehicles, and satellite communications (SATCOM) radomes on various islands.²⁷ Although the EW infrastructure is located in the South China Sea, it poses a larger threat to the region. The HFDF arrays, SATCOM-monitoring radomes, and electronic intelligence (ELINT) systems are far reaching, allowing the PLA to track both civilian and military global navigation satellite system (GNSS) signals.²⁸ These systems offer the PLA advantageous positioning not only across first and second island chains in the Pacific Ocean but also into the Indian Ocean. Unlike traditional wartime ISR, this persistent engagement is not necessarily tied to imminent kinetic conflict. Rather, it allows China to contest information dominance while blurring the distinction between routine exercises and preparatory targeting.

Scenario Assessment

To grasp how a PLA operating under an accelerated kill-chain may look, this paper uses a scenario-based assessment of how such an operation may occur during a gray-zone quarantine of Taiwan. Taiwan provides a useful stress test for examining how non-kinetic kill-chain operations affect crisis stability under gray-zone conditions. The following assessment adopts the scenario from the CSIS China Power Project's *How China Could Quarantine Taiwan*.²⁹ Adopting an established scenario provides a credible foundation for assessing PLA operations in the region and one that is familiar to policymakers. CSIS's scenario also defines phases, reasoning, and decisions that allow this assessment to focus on mapping the EW against Taiwan's systems. Therefore, the assessment can focus on the implications of obscured attribution and escalating pressure within a limited decision cycle.

A gray-zone quarantine is defined as an operation that aims to control maritime or air traffic through law enforcement mechanisms. Unlike a blockade, which utilizes military means to isolate the island, a quarantine

is designed to be coercive while remaining below the threshold of an armed conflict. The Chinese Coast Guard (CCG), China Maritime Safety Administration, and maritime militia consisting of armed fishing vessels are the primary actors for maritime enforcement.³⁰ As the largest coast in the world with “150 ongoing vessels and more than 400 vessels,” the CCG can maintain a constant presence in the Taiwan Strait and surrounding waters.³¹ While international trade could still flow through the Taiwan Strait, China would ultimately decide who and what may approach Taiwan. The purpose of the quarantine is to undermine Taiwan’s ability to operate normally while avoiding escalating into a formal military blockade.

A scenario assessment of a gray-zone quarantine is chosen over a complete blockade of Taiwan for several reasons. First, given the current PLA doctrine, the PLA would seek to disrupt and disable Taiwan’s command, control, and communications (C3) as much as possible before triggering kinetic conflict. Between June 2020 and July 2025, 203 EW and 81 ELINT assets were reported to have violated Taiwan’s Air Defense Identification Zone (ADIZ).³² Therefore, it is important to assess the range of possible actions that could occur. Second, the purpose of a quarantine for China is to evaluate the international community’s tolerance of PLA actions in the Taiwan Strait. This period represents a window in which Taiwan, the United States, and the international community may still effectively de-escalate.

Phase 1: Ambiguous Probing and Attribution Erosion

Phase 1 represents the preparatory phase in which China shapes the environment in its favor before enforcing a quarantine. Prior to any formal announcement, the CCG and fishing militia vessels will conduct limited and reversible disruptions to satellite-based positioning, navigation, and timing (PNT) services in the Taiwan Strait and surrounding airspace. These probes will occur in the weeks leading up to the quarantine to evaluate Taiwan’s interference-detection threshold. The short disruptions would not last more than a day but would be long enough for their effects to be detected in two to ten percent of aircraft operating over Taiwanese cities. Similar effects would occur for vessels transiting throughout the Taiwan Strait, particularly around Taiwan’s major ports. The disruptions would be indiscriminate, causing all vessels in the Strait to experience Automatic Identification System (AIS) timestamp drifting, position jumps, or a brief loss of satellite lock, regardless of nationality.³³

The disruptions during this phase are characterized by being geographically uneven and of short duration. At this level, the disruption is ambiguous enough to be attributed to ionospheric scintillation and other natural space weather disturbances rather than intentional electronic attacks.

During this phase, the PLA Air Force (PLAAF) will frequently fly aircraft near Taiwan’s ADIZ while the PLA Navy (PLAN) deploys vessels carrying electronic support measures capable of detecting GNSS and radar activity. These incursions allow China to map Taiwan’s radar activity and PNT signal environment, including identifying locations of both military and civilian GNSS receivers. At the same time, China will position EW assets closer to Taiwan through aircraft carriers operating in the South China Sea and East China Sea. PLAN surface vessels equipped with jammers will increase their presence in the Taiwan Strait near major ports, such as Taipei and Kaohsiung. South China Sea outposts will increase signal monitoring across the Bashi Channel. An increase in CCG and fishing vessel activity will be reported in the Taiwan Strait, Bashi Channel, and the Senkaku/Diaoyu Islands. The purpose of the phase lies in the information effect on Taiwanese forces. Early PNT interference erodes attribution confidence while forcing Taiwan authorities to determine whether anomalous behaviors reflect routine PLA activities or the beginning of a coordinated campaign. Time is consumed in validating data, narrowing the window for political response.

Phase 2: Quarantine Announcement and Decision-Time Compression

Following the announcement of a law-enforcement quarantine, PNT interference becomes more spatially concentrated and temporally persistent along major air and sea approaches to Taiwan. Law enforcement and maritime militia vessels will be positioned on the edge of Taiwan exclusive economic zone, while PLA forces will be positioned outside. EW-capable aircraft and vessels, such as the Type 052D Class (Luyang III) Destroyer and J-16D aircraft, take positions circling outside Taiwan’s ADIZ, framing their presence as part of routine training or maritime safety operations. Their proximity offers rapid response and the ability to escalate operations if Taiwanese forces or the international community challenges the quarantine.

During this phase, the PLA Cyberspace Force will apply low-level PNT interference to introduce mild but persistent navigational uncertainties for commercial shipping approaching Taiwan’s ports. Ships will now encounter short durations of position drift. These

localized disruptions create a pretext for increased CCG presence, claiming waters around Taiwan are unsafe due to “maritime hazards.” Chinese fishing vessels can reinforce this narrative by positioning themselves along shipping routes, simultaneously creating the appearance of congestion and collision risks. The CCG will warn vessels that sailing closer to Taiwan risks collision and will direct vessels away from Taiwan ports, thereby reinforcing the quarantine. Similarly, PLAAF EW aircraft will degrade the reliability of air navigation in selected air corridors, aligning with major airports. This generates enough risk for airlines to comply with China’s Air Traffic Management Bureau (ATMB) suggested reroutes, while the persistent presence of PLAAF aircraft will reinforce the new air routes.

During this phase, the PLA’s EW functions as leverage for its actions in the region. Civilian and military vessels and aircraft must make decisions earlier with less reliable information or risk collision. As China’s measures gain more credibility through compliance, Taiwanese forces will attempt to deploy air and maritime forces to restore situational awareness and condemn PLA actions. The ROC Air Force, Navy, and Coast Guards may conduct operational exercises near PLA-operated regions to investigate maritime and airspace activities. However, there are drawbacks. First, as the CSIS scenario reports, Taiwan’s Coast Guard is severely outnumbered by the CCG, with only “10 oceangoing ships and approximately 160 smaller vessels.”³⁴ Therefore, obtaining coherent situation awareness for the entire Strait is difficult. Second, the ambiguity surrounding the source and intent of the disruptions is intentionally left unsaid to complicate a proportional response. Actions that seem forceful, such as large-scale deployment of ROC forces, risk escalation. However, restraint risks acquiescing, further hindering ROC forces’ decision making due to intermittent disruptions.

Phase 3: Sustained Non-Kinetic Pressure and Escalation

Once commercial and civilian control of air and sea corridors, China will actively enforce the quarantine with a persistent and assertive presence. EW activity becomes integrated across multiple domains, producing sustained degradation of PNT systems rather than isolated disruptions. Navigation uncertainty affects not only commercial traffic but also military patrols, ISR systems, and command-and-control synchronization across domains. In this phase, China’s objective is to make noncompliance difficult and increasingly dangerous. The CCG and China’s Air

Traffic Management Bureau will enforce new sea and air corridors by allowing a limited number of vessels and aircraft through in order to maintain the image of safety.

Simultaneously, the PLA will conduct coordinated EW in multiple methods. The PLA will employ GNSS spoofing against ROC forces’ military and dual-use receivers. ROC forces will begin to see misreadings of position and altitude. The PLA Cyberspace Forces will launch cyberattacks on telecommunication timing servers, disrupt timing and synchronization networks, and further slow command-and-control. As Taiwan’s situational awareness continues to degrade, China will escalate its PNT disruptions through reversible counterspace capabilities. These measures may include jamming GPS downlink signals to disrupt navigation services over Taiwan, the East China Sea, and parts of the South China Sea or conducting uplink jamming from ground-based jammers that interfere with command-and-control. In addition, Chinese ground-based laser stations might use high-powered lasers to temporarily blind and dazzle commercial Earth-observation satellites, further preventing Taiwan from gaining situational awareness.

At this point in the quarantine, escalation risks become increasingly system generated. Taiwanese forces, seeking to restore situational awareness and deterrence credibility, face incentives to accelerate their own response processes. Measures might be taken to compensate for greater uncertainty and further compress decision windows on all sides. China leverages this against Taiwan to increase maritime enforcement and announces this to the international community.

Implications for Crisis Stability in the Gray Zone

The scenario demonstrates the implications for crisis stability in this version of the PLA kill chain. It suggests that instability may arise in the absence of first-strike incentives and deliberate brinkmanship. Instead, instability can emerge endogenously from the interaction between information degradation, adaptation, and decision cycle compression. Classic literature of crisis stability emphasizes incentives to act quickly when actors fear being disarmed by an opponent’s first move or believe that delaying action worsens their strategic position. In this scenario assessment, neither condition is present in a conventional sense. Neither side seeks escalation, and neither possesses reliable information indicating that armed conflict has become unavoidable. The pressure, instead, to act increases regardless as electronic warfare degrades situational

awareness and reduces confidence in the stability of operational conditions. Rather, it suggests that crisis instability can be driven by information decay rather than solely by adversary intent. While adaptations in this scenario could partially restore the systems' functionality, they do not restore pre-crisis conditions of deliberation and control. Instead, each round of adaptations shortens the time between action and response. Thus, stability depends on whether recovery restores sufficient temporal and cognitive margins for signaling, assessment, and restraint. In gray-zone competition, resilience that accelerates interaction tempo may paradoxically increase escalation risk even when it succeeds tactically.

Policy Implications for U.S. Crisis Stability

Although the operational effects described in the scenario are based on a Taiwan scenario, the assessment offers strategic significance in illustrating PLA capabilities integrating electronic warfare into their automated kill chain. China's integrated kill chains and electronic warfare undermine U.S. crisis stability by reshaping the information environment in which United States leaders make escalation decisions. Policy responses that focus solely on mirroring the PLA's speed and integration risk reinforcing crisis instability. Therefore, U.S. policymakers should prioritize preserving decision space and maintaining control over escalation under conditions of persistent interference.

The United States' current initiatives emphasize rapid data fusion and responsiveness in contested environments through initiatives such as Project MAVEN and the Replicator Initiative.³⁵ However, these efforts can accelerate uncertainty during gray-zone crises. The Department of Defense should require that automated systems demonstrate how they perform under degraded conditions through clear evaluation criterion. These criteria should include the ability to slow, pause, or revert automated processes when confidence thresholds decline. In addition, there is a need to institutionalize human-around-the-loop escalation controls. While automated systems can efficiently support sensing, correlation, and tasking, escalation judgement requires interpretation of domain conditions. U.S. operational policy should specify which conditions may remain automated during contested conditions and which require human validation, particularly when automated outputs could trigger cross-domain responses. Establishing crisis-mode operating procedures that decouple automated sensing and targeting from escalation would reduce the

risk that information degradation turns into military pressure.

Operational planning should also include both rapid recovery and sustained performance across multiple cycles of disruption and response. As the scenario assessment illustrates, instability is most likely to emerge not during an initial electronic attack, but through repeated interference and adaptation that erodes operational functionality. Therefore, the United States should conduct joint exercises and wargames with Indo-Pacific partners to model multi-cycle electronic warfare campaigns. The purpose of these exercises and wargames is to assess initial recovery and after adversaries adapt and retarget. This can be achieved through both Track 1.5 and Track 2 diplomacy with partners in the region.

Finally, U.S. crisis management efforts should more directly address the destabilizing effects of persistent electronic warfare in gray-zone competition with China. Existing military communication mechanisms are poorly suited to managing incidents involving ambiguous interference, anomalous system behavior, or degraded situational awareness. The United States should pursue dialogue and confidence-building measures focused on electronic warfare interactions, including shared understandings of interference categories and mechanisms for clarifying incidents affecting navigation, sensing, or command-and-control systems. While such measures are unlikely to deter gray-zone activity outright, they can help slow escalation dynamics and preserve time for assessment during periods of sustained competition.

Limitations

While the scenario assessment highlights dynamics relevant to the U.S.-China military competition, the paper acknowledges some limitations in the scope of the analysis. The scenario assessment assumes that both China and the United States seek to avoid large-scale kinetic escalation and instead operate below the threshold of open war through persistent electronic interference, signaling, and operational pressure. As a result, the paper does not assess how automated kill chains or electronic warfare would function once kinetic hostilities begin, nor does it evaluate warfighting effectiveness or operational outcomes under conditions of sustained combat. The argument is instead focused on the pre-conflict and early-crisis phase, where ambiguity, attribution challenges, and escalation management play a central role in shaping decision-making. The dynamics identified here should therefore be understood as most relevant to periods of

heightened tension rather than to mobilized warfare. The assessment also assumes that both China and the United States seek to avoid large-scale kinetic escalation and operate below the threshold of open war through persistent electronic interference, signaling, and operational pressure. As a result, the paper does not assess how automated kill chains or electronic warfare would function once kinetic hostilities begin, nor does it evaluate warfighting effectiveness or operational outcomes under conditions of sustained combat. The argument is instead focused on the pre-conflict and early-crisis phase, where ambiguity, attribution challenges, and escalation management play a central role in shaping decision-making. The dynamics identified here should therefore be understood as most relevant to periods of escalated tension rather than to mobilized warfare.

The scenario intentionally does not consider political and strategic variables that would shape crisis behavior. Domestic political considerations and alliances are important but would muddle the overall purpose of the scenario. Similarly, the analysis does not model the role of U.S. decision making in detail, focusing instead on how automated kill chains and electronic warfare affect the broader crisis environment in which U.S. leaders would operate.

The scenario involving Taiwan represents a most-likely case for the gray-zone competition and crisis stability with electronic warfare and gray-zone activities short of war. However, the instability generated by repeated information degradation and adaptation may be relevant in other scenarios in the Indo-Pacific region. However, the report does not seek to evaluate the military effectiveness of either the United States or China. The purpose is to examine how automated kill chain integration and persistent electronic warfare shape crisis dynamics through information dominance. Therefore, the focus of the report is on crises evolving under conditions of sustained interference even when restraint is preferred.

Conclusion

The PLA's use of automated kill chains and persistent electronic warfare represents a new fog of war. This report seeks to demonstrate how instability can emerge through repeated cycles of information degradation and decision-cycle compression. In environments where sensing, navigation, and communications are persistently contested, automated processes intended to enhance operational effectiveness can also accelerate confidence in situational awareness and result in

unintended escalation. The scenario centered on the Taiwan Strait demonstrates how that might play out. Although Taiwan represents a specific case of operational exposure to automated kill chains and EW interaction, information degradation and rising escalation pressures may emerge anywhere. Thus, this report and its conclusions should be understood as a warning rather than a prediction. It does not suggest that crisis instability is inevitable, nor does it imply that the United States or allied forces lack the capacity to adapt. Rather, it highlights how existing operational concepts, if focused narrowly on speed, integration, and recovery, may underestimate the cumulative effects of persistent interference on decision-making and escalation control. For U.S. policymakers, the Taiwan scenario provides a demonstration of broader challenges that will impact the United States operationally. Without explicit attention to decision-cycle preservation and escalation control, efforts to maintain stability may inadvertently reinforce destabilizing dynamics. As competition intensifies in domains where interference is persistent and attribution is uncertain, stability will depend less on deterring individual actions and more on shaping how interactions develop over time.

Military Parade (China Aerospace Studies Institute, Air University, September 22, 2025), 1, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2025-09-22%202025%20Military%20Parade%20Information%20Operations%20Group.pdf?ver=brvVqMOj7RcC1V_Nc3aTLg%3d%3d

¹⁹ Katarina Radoš, Marta Brkić, and Dinko Begušić. 2024. “Recent Advances on Jamming and Spoofing Detection in GNSS.” *Sensors* 24, no. 13: 4210. <https://doi.org/10.3390/s24134210>.

²⁰ Katarina Radoš, Marta Brkić, and Dinko Begušić. 2024. “Recent Advances on Jamming and Spoofing Detection in GNSS.”

²¹ “JN-1105 Chinese Portable Communications EW Complex,” Operational Environment Data Integration Network (ODIN), <https://odin.tradoc.army.mil/WEG/Asset/c780172bc4beb3bfa71eda88e2da46e8>

²² J. Michael Dahm, Special Mission Aircraft and Unmanned Systems, South China Sea Military Capability Series (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, October 2020), <https://apps.dtic.mil/sti/trecms/pdf/AD1128646.pdf>.

²³ Ibid.

²⁴ Ibid.

²⁵ Ibid.

²⁶ Guo Yuandan, Liu Xuanzun, and Leng Shumei, “PLA’s J-16D electronic warfare aircraft spotted for 1st time near Taiwan,” *Global Times*, January 25, 2022. <https://www.globaltimes.cn/page/202201/1246818.shtml>.

²⁷ Asia Maritime Transparency Initiative, “China’s Spratly ISR and EW Upgrades,” December 2, 2025, <https://amti.csis.org/chinas-spratly-isr-and-ew-upgrades/>; Dahm, J. Michael. Special Mission Aircraft and Unmanned Systems.

²⁸ Richard L. Bernard, *Electronic Intelligence (ELINT) at NSA* (Center for Cryptologic History, National Security Agency, 2009), 1, <https://www.nsa.gov/portals/75/documents/about/cryptologic-heri->

[tage/historical-figures/publications/publications/misc/elint.pdf](https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures/publications/publications/misc/elint.pdf)

²⁹ Bonny Lin, et al., How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios (Washington, D.C.: CSIS, June 2024), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240605_Lin_Taiwan_Quarantine_0.pdf

³⁰ Ibid, 4.

³¹ Ibid.

³² Gerald C. Brown, Benjamin Lewis, Taiwan ADIZ Violations, PLATracker, Taiwan ADIZ Violations Tracker, 2026. https://docs.google.com/spreadsheets/d/1qbfY-F0VgDBJoFZN5elpZwNTiKZ4nvCUcs5a7oYwm52g/edit?gid=2051_027998#gid=2051027998

³³ U.S. Coast Guard Navigation Center, “Automatic Identification System (AIS) Overview,” *Navigation Center, U.S. Coast Guard*, <https://www.navcen.uscg.gov/automatic-identification-system-overview>.

³⁴ Bonny Lin, et al., How China Could Quarantine Taiwan: Mapping Out Two Possible Scenarios.

³⁵ Robert O Work. 2017. “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven).” Memorandum, Department of Defense, April 26, 2017. <https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf>; Ryan McCormack. “The Replicator Initiative Is Key to the Army’s Modernization.” *Brookings Institution*, December 20, 2023. <https://www.brookings.edu/articles/the-replicator-initiative-is-key-to-the-armys-modernization/>.