

IMPACT OF UNMANNED SYSTEMS TO ESCALATION DYNAMICS

Unmanned systems are proliferating at an explosive pace, and the U.S. Navy is increasingly employing and encountering them. Despite their many benefits, unmanned systems create the potential for unanticipated second-order effects. Of particular concern is the potential for unmanned systems to alter escalation dynamics between states, increasing risks to militaries and states. In light of this, CNA examined the impact of unmanned systems to escalation dynamics, focusing on how near-term unmanned systems (2017-2025) affect state-on-state competition in the maritime domain during shaping and deterrence operations.

Unmanned systems are not equivalent to manned systems as a result of three key distinctions: First, unmanned systems differ in their concepts of employment, relying heavily on remote communications, automation, or autonomy. Second, the lack of manning affects how a system is valued. This, in turn, influences acceptable level of risk during employment, willingness to protect systems, and willingness to counter foreign systems. Third, unmanned systems—unconstrained by biological factors such as space for personnel, endurance, and G-force restrictions—introduce novel capabilities, for which operating norms are not yet established. This can enable novel missions, as well as new opportunities to conduct covert or less-attributable operations.

To understand the impact of unmanned systems to escalation dynamics, CNA conducted an in-depth review of unmanned systems operations. Ultimately, we identified the following ways that unmanned systems affect escalation dynamics:

- 1. Unmanned systems can increase the potential for *deliberate* escalation. They provide novel options to take deliberately escalatory actions. And with no direct risk to personnel, they may increase the willingness of actors to employ these options.
- 2. Unmanned systems can increase the potential for *inadvertent* escalation. Operating norms for new systems take time to establish. New escalation thresholds for unmanned systems are evolving, and existing thresholds are ambiguously understood when applied to unmanned systems. Illustrating this, in 2016 China captured a U.S. unmanned undersea vehicle, asserting it posed a "hazard to navigation." The U.S. challenged the action as "unlawful," claiming the UUV was a "sovereign immune vessel." Without commonly held norms or a clear understanding of the policies, values, and priorities of a potential adversary, forces deploying and encountering unmanned systems could inadvertently cross escalation thresholds.
- 3. Unmanned systems can increase the potential for accidental escalation. Unmanned systems, remotely or autonomously controlled, create reliability concerns that can result in accidentally crossing an adversary's escalation threshold. This may include unintended offensive actions or navigation into sensitive territory or close to foreign forces. Similarly, manned forces reacting to a foreign unmanned system may lack an understanding of how to apply tactical guidance, such as pre-planned defensive responses, if that guidance is vague, unpracticed, or not updated to account for new technologies.
- 4. Unmanned systems can increase the potential for internal errors of coordination and communication. Without good internal communication and coordination, a state's tactical actions may not align with its strategic intentions, increasing the chances for unintended escalation. New processes for coordinating unmanned systems operations will be necessary. Remotely operated unmanned systems may require coordination with operators outside of theater who are less familiar with theater guidance, and the reduced risk to personnel can lead to less scrutiny of operators controlling unmanned systems. Autonomous systems may require entirely novel means in order to interpret commander's intent.
- 5. Unmanned systems can make actors either more or less likely to rationally consider escalatory consequences. On the one hand, actors may exhibit less concern about crossing escalation thresholds when employing or countering unmanned systems, failing to consider that escalation may affect more than just that unmanned system. On the other, actors may also exhibit tactical patience when protecting unmanned systems. When lives are not immediately on the line, they may be more willing to accept the risk of hostile action.

6. Unmanned systems can either positively or negatively affect the likelihood that an action will provoke an escalatory response. Certain unmanned systems may avoid a response by operating undetected or without clear attribution to a state. Used overtly, however, unmanned systems may more readily provoke a response. The likelihood of a counter-response by the deployer of the unmanned system—after a system is attacked or captured—is also influenced by the unique attributes of unmanned systems. For example, the absence of human casualties eliminates the need for personnel recovery missions and reduces pressure for retaliation, though the technology's value or sensitivity may warrant action to recover or destroy it.

Military operations involving unmanned systems must account for these shifting escalation dynamics. Operational experience to date demonstrates that a policy and guidance gap is already affecting U.S. Navy operations involving unmanned systems. Additionally, future U.S. operating concepts increasingly rely upon unmanned systems, and include an underlying assumption that freedom of action for unmanned systems can be established and ensured. Whether this assumption will hold remains to be seen.

We urge the U.S. to adopt a consistent, strategic approach to unmanned systems development, employment, protection, and encounters. Wittingly or not, U.S. behavior is laying the groundwork for international norms that will govern future military operations, and it is important that the U.S. engage in deliberate efforts to influence the establishment of predictable and desirable international operating norms for unmanned systems. A more deliberate approach will require the U.S. to clarify the international legal basis and behavioral standards that it supports for the military employment of unmanned systems. The military will also need to align operational guidance with those desired standards and clarify how rules of engagement and pre-planned responses apply to unmanned systems. At the same time, operational commanders must be prepared for the reality that international norms and legal regimes for unmanned systems are immature, and that the existing escalation thresholds of other states may be different from what the U.S. desires or expects.

CNA CENTER FOR AUTONOMY AND AI

CNA's Center for Autonomy and AI supports the U.S. goal of effectively incorporating autonomy, AI, and related technologies into military capabilities. Autonomy and AI represent revolutionary technologies in warfare which offer opportunities to the U.S. for countering and deterring emerging threats, addressing security challenges and advancing U.S. national interests. But this opportunity is by no means certain, since autonomy also offers potential asymmetric advantages to near-peer competitors, some of which have been pursuing these capabilities aggressively. Likewise, rapid innovation in the private sector and a commercial research and development sector dwarfing that of the U.S. military create new challenges for the U.S., which will need to quickly identify and integrate cutting edge technological developments in this rapidly changing environment.

Because of the foundational impact autonomy and artificial intelligence will have on the character of warfare, CNA created the Center for Autonomy and Artificial Intelligence to focus on these emerging technologies and their contribution to national security. The Center capitalizes on the ability to leverage the scientists and analysts of CNA's staff of nearly 700, with their experience base in military operations, test and evaluation, security and intelligence analyses, technology assessment, and autonomy and AI.

ABOUT CNA CORPORATION

CNA is a not-for-profit research and analysis organization with 75 years of experience providing government agencies with datadriven insights and real-world, actionable solutions grounded in our direct experience with the operational environments where these solutions are applied. CNA developed the foundational techniques for operational analysis to address complex challenges facing government programs. We have applied these techniques successfully in areas ranging from defense to aviation, education, justice, and homeland security. For more information please contact: Dr. Larry Lewis, Director, Center for Autonomy and AI 703-824-2020 Lewisl@cna.org

Dr. Anna Williams, Research Scientist 703-824-2748 williamsa@cna.org