RESEARCH SUMMARY

Disrupting Deterrence

Examining the Effects of Technologies on Strategic Deterrence in the 21st Century

MICHAEL J. MAZARR, ASHLEY L. RHOADES, NATHAN BEAUCHAMP-MUSTAFAGA, ALEXIS A. BLANC, DEREK EATON, KATIE FEISTEL, EDWARD GEIST, TIMOTHY R. HEATH, CHRISTIAN JOHNSON, KRISTA LANGELAND, JASMIN LÉVEILLE, DARA MASSICOT, SAMANTHA MCBIRNEY, STEPHANIE PEZARD, CLINTON REACH, PADMAJA VEDULA, EMILY YODER

To access the full report, visit www.rand.org/t/RRA595-1

ISSUE

In this report, the authors examined the implications of eight specific emerging technologies for both the effectiveness of U.S. deterrent policies and the stability of deterrence relationships.

APPROACH

The authors reviewed U.S. government strategy documents to define the deterrence requirements of U.S. national security strategy. They reviewed existing literature on deterrence, escalation, and strategic stability to develop criteria against which to measure the effects of technologies. They evaluated Chinese and Russian views of the nature of deterrence and their perceptions of emerging technologies. For the technology analysis, the authors identified eight technology areas for closer examination and conducted in-depth assessments of the current status and emerging potential of each. Finally, they employed four lines of analysis to generate possible causal relationships among the eight technology areas and deterrence outcomes.

CONCLUSIONS

The research highlights two overarching conclusions. First, taken as a group, collections of emerging technologies—especially in the realms of information aggression and manipulation, automation, hypersonic systems, and unmanned systems—hold significant implications for both the effectiveness and stability of deterrence. These risks may call for changes in U.S. policies, operational concepts, and technology development programs. Second, an emerging transition to new ways of warfare, empowered by these same emerging technologies, poses more-general risks to U.S. deterrent policies than does any single technology. If the United States is left behind in the technological, conceptual, and doctrinal transition to this new era, both the effectiveness and stability of U.S. deterrent policies are likely to suffer. In addition, the research generated more-specific findings, including the following:

- Individual technologies are typically an enabler, not a prime cause, of deterrence failure. Improved capabilities at the margins are rarely if ever decisive factors in deterrence failure.
- The risks of deterrence failure are greatest in scenarios in which multiple technologies work together to exacerbate classic sources of deterrence failure—which may be precisely the scenario set to emerge over the next two decades.

continued

- Technology combinations complicate deterrence by offering the potential to hit multiple targets across many attack surfaces simultaneously. This creates an opportunity for society-wide paralytic attacks that could undermine deterrence by allowing an aggressor to believe that it could freeze the defender long enough to achieve its desired gains.
- Technologies have the greatest potential to degrade the effectiveness of deterrence in scenarios involving China. The cases in which technology poses a more realistic threat to the effectiveness of U.S. deterrent threats are largely limited to two contingencies involving China: Taiwan and the South China Sea.
- Multiple, interacting forms of automation carry very significant risks, especially for the stability of deterrent relationships.
- Many technologies challenge the U.S. ability to deter aggression, coercion, and influence-seeking below the threshold of major war. Cyber capabilities, disinformation, unmanned systems, biological tools, and even artificial intelligence (AI)–driven decision support systems (DSSs) could strengthen and increase the frequency of bellicose actions in the gray zone.
- There is a growing potential for information-manipulation technologies, including deepfakes, to contribute to the failure of deterrence.
- On the opportunity side of the ledger, the United States could employ emerging technologies to enhance the effectiveness and stability of deterrence in multiple ways. These include investments in resilience against systemic attack and counter–systems warfare; the use of drone, AI-driven analysis, and cyber capabilities as part of a network of persistent, comprehensive domain awareness and targeting capabilities; networks of new-generation precision-guided weapons married to unmanned aircraft systems (UASs) and DSSs to intensify the threat to any advancing forces; and the transfer of technology, including co-development, to allies and partners to enhance their capabilities to deter and defeat aggression.

RECOMMENDATIONS

Using these findings, the authors offer specific implications for the Air Force:

- To remain attuned to deterrence risks, focus first on understanding the perceptions of rivals and second on the technology.
- The Air Force should place special emphasis on awareness of both the technology packages in which near-peer adversaries are investing and how they seek to combine them.
- Securing against information network or Chinese "system destruction" attacks is a precondition for effective deterrence and stability.
- The UAS and counter-UAS competition is likely to become a major focus of U.S. defense investments and the stability of deterrent relationships in key theaters.
- Norms, rules, and limits governing technologies could benefit the United States.
- Building relationships with rival air force leaders can provide important benefits.
- Technology integration in support of concepts of warfare will be increasingly crucial.
- The United States will gain significant competitive advantage if it can expand multilateral development of priority systems—including sensing, unmanned aircraft, and precision weapon—for partner or ally self-defense.

RAND PROJECT AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. For more information, visit PAF's website at www.rand.org/paf.