



JAMES RYSEFF, CHIA-HSI JESSICA LIN, D. SEAN BARNETT, MICHAEL BOHNERT, CALEB LUCAS,
BARRY WILSON, JIM MITRE

Harnessing the Power of Private Sector Innovation to Defeat a Chinese Invasion of Taiwan

Relighting Vulcan's Forge

This publication has completed RAND's quality-assurance process but was not edited.

For more information on this publication, visit www.rand.org/t/RRA2930-1.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

© 2024 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

About This Report

Harnessing the power of private sector innovation is seen as an essential way to help the United States maintain its technical advantage over its competitors. In this spirit, the Special Competitive Studies Project asked RAND to bring together private sector technologists with defense experts to brainstorm technological solutions that could help the United States and Taiwan defeat a Chinese invasion. In total, the group identified seventeen technological solutions across six categories that would be both technologically feasible in the short term and would provide a meaningful benefit to the United States and its partners.

RAND National Security Research Division

This research was sponsored by the Special Competitive Studies Project and conducted within the International Security and Defense Policy Program of the RAND National Security Research Division (NSRD). NSRD conducts research and analysis for the Office of the Secretary of Defense, the U.S. Intelligence Community, the U.S. State Department, allied foreign governments, and foundations.

For more information on the RAND International Security and Defense Policy Program, see www.rand.org/nsrd/isdp or contact the director (contact information is provided on the webpage).

Acknowledgments

We wish to thank our sponsors at the Special Competitive Studies Project, Ylber Bajraktari and Justin Lynch. We also wish to thank our reviewers, Dave Ochmanek and Emelia Probasco, for all their helpful comments and inputs. Finally, we wish to thank all of our participants in our exercises for their time and ideas.

Contents

About This Report.....	iii
Contents	iv
Executive Summary	1
Background	4
Methods.....	6
Technological Solutions.....	8
Core Technical Infrastructure	8
Command and Control	12
Intelligence Collection and Analysis	19
Unmanned Systems.....	22
Applications to Improve Training.....	28
Logistics.....	31
Analysis of the Impact of the Technological Solutions	34
Assumptions for Evaluation.....	34
Evaluative Approach.....	35
Major Impacts of the Technological Solutions	36
Conclusions and Recommendations.....	38
Abbreviations	40
References	41

Executive Summary

Over the past decade, American policymakers and defense experts have become increasingly concerned about the improving military capabilities of the People's Republic of China (PRC). The Biden Administration's 2022 National Security Strategy recognizes that the PRC is America's only rival with "both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it"¹ and senior American military leaders have begun voicing concerns that China's military might attempt to invade Taiwan by 2027 or even earlier.² One way the Department of Defense (DoD) hopes to counter the rising threat from China is by leveraging the American private sector and its enduring strength in technological innovation. DoD's leadership hopes that this will reinvigorate America's traditional technological advantage which has been eroding over time.³

In line with this strategy, the Special Competitive Studies Project asked the RAND Corporation to organize a series of table top exercises bringing together innovative technologists from the private sector along with DoD personnel and other defense experts. The purpose of these exercises was to generate a set of technological solutions which could be fielded to warfighters in the 2027 timeframe and that had the potential to have a game-changing impact on the ability of the United States and Taiwan to repel a Chinese invasion attempt. While some of these solutions are not novel, the priority was to identify solutions which could feasibly be implemented in the timeframe and which could make a significant impact on the conflict. To accomplish this, RAND and SCSP recruited technologists from a variety of private sector companies. Some participants worked at large technology firms with extensive experience working on cutting edge technologies. Other participants came from the smaller startup corporations that have often proved to be the lifeblood of American innovation. Finally, other participants worked in innovation groups at traditional defense contractors. RAND also invited the participation of a range of DoD technical and military experts.

The first exercise in our series focused on familiarizing these technologists with the problems and challenges the Defense Department faces when attempting to defeat a Chinese invasion of Taiwan. RAND conducted an unclassified wargame depicting a Chinese invasion of Taiwan set in 2027 with both current and former DoD personnel commanding Blue (US) and Green (Taiwan) forces against experts on the Chinese military commanding the Red (China) side.

¹ The White House, *National Security Strategy*, October 2022.

² Sam LaGrone, "Milley : China Wants Capability to Take Taiwan by 2027, Sees No Near-term Intent to Invade", *USNI News*, June 23, 2021.

³ DoD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018

Having established this context, RAND then organized a second event in San Francisco where teams comprised of technologists and DoD personnel brainstormed potential technological solutions to solve the operational problems they had observed. The participants discussed the technological aspects of each idea and assessed the maturity and feasibility of the technologies involved. To conclude, RAND brought these participants together again for one final exercise at its Washington DC office. In this exercise, participants focused on further defining the operational context these technological solutions would be employed in and exploring the warfighting impact that each solution could make. At the end of the event, a “shark tank” of experts heard pitches from the participant teams for each of the solutions and provided feedback to the participants. Ultimately, our participants generated 17 different technological solutions across 6 operational categories: core technical infrastructure, command and control, intelligence collection and analysis, unmanned systems, improved training, and logistics.

To evaluate the potential impact of these solutions, RAND updated its adjudication of the wargame conducted in the first exercise to incorporate the technological solutions generated by our exercise. Although this analysis applied fairly low-resolution tools and is thus not definitive, it points to three major impacts. First, the technological solutions increased losses inflicted on China’s amphibious forces from approximately half (in the unmodified game) to two-thirds (after incorporating the additional technological solutions). Second, the combined effects of the added technological solutions caused China’s air assault forces to lose an additional 10 percent of their overall strength compared to the losses incurred in the original game. Finally, the technological solutions reduced US fighter aircraft losses during the first week of the war by approximately half while increasing Chinese fighter losses by approximately 70 percent. All in all, RAND’s analysis found that the technological capabilities could plausibly make a meaningful difference in the outcome of the wargame scenario.

As a result of our analysis and experiences during the project, we draw three conclusions.

- The Defense Department should engage in more immersive outreach efforts to innovators in the private sector to better contextualize military operations. DoD should shift these discussions away from describing detailed requirements for specific solutions to describing the problems and challenges faced by U.S. and allied forces in specific scenarios. Doing so in a manner where technologists have a better understanding of the broader operational context and access to operators and “end users” for frank exchanges can enable technologists to imagine and discover the best solutions to solve them. This approach would follow best practices established by the private sector.⁴
- This series of exercises demonstrates that technological solutions exist which could both be deployed to warfighters at scale in the short term (next 3-5 years) with minimal technological risk and which could meaningfully enhance America’s ability to defend against Chinese aggression in the Indo-Pacific theater. While we do not claim that the set

⁴ Marty Cagan, *Inspired: How to Create Tech Products Customers Love*, John Wiley & Sons, 2017, p. 29; Eric Ries, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, Crown Business, 2011.

of solutions generated by our exercises is either optimal or exhaustive, the outcome verifies that progress is possible.

- Several of the technological solutions generated by this project demonstrated the potential to have a game-changing impact on a future conflict over Taiwan. In particular, improved smart munitions have the potential to inflict significant losses on both the seaborne and airborne components of the invasion force, and improved decoys and deception techniques could substantially decrease American losses of fighter aircraft. At the same time, many of these technological solutions have a less direct and less quantifiable impact on battlefield outcomes. Improvements in core infrastructure, situational awareness, command and control, and training of Taiwan reserve forces to improve their competence and will-to-fight could yield meaningful - if non-deterministic – benefits on the battlefield. In particular, many of the greatest improvements from these solutions provide an information advantage for U.S forces over their adversaries, a factor that could prove key to any future conflict.

Although building out any of these ideas from the initial concept into a finished product would require additional analysis and iterative development to perfect, they each have the potential to meaningfully assist American and allied warfighters in defeating their future adversaries.

Background

Over the past decade, American policymakers and defense experts have become increasingly concerned about the improving military capabilities of the People's Republic of China. The Biden Administration's National Security Strategy recognizes that the People's Republic of China is America's only rival with "both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."⁵ American military leaders are concerned that this rising national power may ultimately be applied to enabling the Chinese military to invade and seize the island of Taiwan. The Chairman of the Joint Chiefs of Staff has testified that the Chinese military has been ordered to be prepared to conquer Taiwan by 2027⁶ and American wargames frequently focus on whether American and Taiwan forces can repel a Chinese invasion.⁷

As the Chinese military has rapidly improved its readiness and equipment, America's ability to improve its own forces has all too often become trapped in the quagmire of its defense acquisition process. In 2016, the leadership of the Senate Armed Services Committee declared "An acquisition system that takes too long and costs too much is leading to the erosion of America's defense technological advantage ... In short, our broken defense acquisition system is a clear and present danger to the national security of the United States."⁸ The 2022 National Defense Strategy concurs with this diagnosis, noting that "Our current (acquisition) system is too slow and too focused on acquiring systems not designed to address the most critical challenges we now face."⁹

To rectify these difficulties, the Department of Defense hopes to draw from the enduring strength of America's vibrant and innovative private sector¹⁰. In that spirit, the Special Competitive Studies Project asked the RAND Corporation to conduct a series of exercises

⁵ The White House, *National Security Strategy*, October 2022.

⁶ Sam LaGrone, "Milley : China Wants Capability to Take Taiwan by 2027, Sees No Near-term Intent to Invade", *USNI News*, June 23, 2021.

⁷ David Ochmanek and Michael O'Hanlon, "Here's the Strategy to Prevent China from Taking Taiwan", *The Hill*, December 8, 2021.

CSIS, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*, January 9, 2023.

CNAS, *Dangerous Straits: Wargaming a Future Conflict over Taiwan*, June 15, 2022.

⁸ United States Senate Committee on Armed Services, "Senate Armed Services Committee completes markup of National Defense Authorization Act for Fiscal Year 2016", press release, May 14, 2015.

⁹ DoD, *2022 National Defense Strategy of the United States of America : Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*, October 27, 2022.

¹⁰ DoD is also taking steps to improve its ability to leverage private sector innovation. These include both reforms to its acquisition processes as well as increasing its outreach efforts to the private sector through offices charged with accelerating innovation.

partnering technologists from some of America's most innovative private sector companies alongside military personnel and defense experts. The participants were tasked with identifying technological solutions which could substantially improve the performance of American and Taiwan forces in repelling a Chinese invasion and which could be deployed to warfighters by 2027. The remainder of this report discusses how RAND recruited these participants and structured the exercises, describes the solutions generated by the participants, discusses the potential impact these solutions could have in defeating a Chinese invasion of Taiwan, and summarizes the takeaways from these exercises.

Methods

The purpose of this project was to bring together technologists from the private sector and national security experts (uniformed military personnel, DoD civilians, and other defense experts) in order to explore technological solutions that could improve the ability of both the United States and Taiwan defend against a Chinese invasion. We recruited technologists for this exercise from a variety of private sector companies. Some participants came from large technology companies that are leaders in advanced software technologies such as artificial intelligence and cloud computing. Other participants came from the smaller and younger startups which have often innovated the most quickly within the US tech ecosystem. Finally, some of our participants came from innovation groups at traditional defense contractors. We partnered these technologists with defense experts – from both the United States and Taiwan - with deep expertise across all of the military services and in all of the major challenges the United States faces when considering how to defeat a Chinese invasion of Taiwan.

RAND structured the series of exercises to have three components. At our first event, the participants witnessed a wargame simulation depicting a Chinese invasion of Taiwan in 2027. The game was held at the unclassified level to allow a wider range of potential private sector participants. A retired US military officer led the command of American and Taiwan forces while RAND experts played the Chinese. A total of 6 DoD personnel and 24 technologists attended this game.

The purpose of this game was to familiarize the technologists with the problems that DoD faces in attempting to defeat large-scale aggression against Taiwan. Best practices from the private sector emphasize that engineering teams are most effective at creating new technological solutions when they are given a problem to solve as opposed to a solution to build¹¹. While this differs from the way DoD's acquisition process typically works, the private sector approach has historically yielded more effective products and capabilities¹². The wargame also established a baseline for assessing the potential impacts of the tech solutions on the outcome of the conflict. In total, the first game identified ten significant operational problems for DoD: Situational Awareness, Detection and Targeting, Command and Control, Information Sharing with Taiwan, Coordination of Military Operations, Fires, Survivable Logistics, Base Resilience, Supporting Taiwan's Will to Fight, and Supporting the Global Information Fight.

¹¹ Marty Cagan, *Inspired: How to Create Tech Products Customers Love*, John Wiley & Sons, 2017, p. 29; Eric Ries, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, Crown Business, 2011.

¹² Defense Innovation Board, *Software Acquisition and Practices (SWAP) Study*, 2019

For the second event, RAND held a structured brainstorming exercise designed to generate technological solutions that could help solve the problems the technologists observed during the wargame. RAND and SCSP selected six of the operational problems to focus on : Situational Awareness; Detection and Targeting; Command and Control; Information Sharing; Coordination of Military Operations; and Survivable Logistics. The participants were split into six groups, each focusing on a different one of these operational problems. In the initial brainstorming phase, a total of 82 ideas were generated. Each team then chose the 3 or 4 ideas they believed were the most promising. The groups spent the remainder of the exercise describing those solutions in greater detail, assessing their technical feasibility, and considering the potential difficulty of integrating the solution into DoD's operations. The teams were asked to only consider ideas the group consensus found to be feasible in the 2027 timeframe. This process generated a total of 19 refined ideas.

At the last event, the participants focused on considering how these technological solutions would actually impact DoD's operations. In order to gauge the potential effects of these solutions, each needed a clear explanation of who would use the solution, how it could be used, and what effects it would be expected to achieve. For this event, the participants were split into three groups and each group explored five technological solutions (or pairs of technological solutions whose use overlapped significantly) in greater depth. The final exercise culminated with a 'Shark Tank' style pitch meeting where the technologists presented their ideas to a panel of retired senior military officers, former senior DoD officials, and a senior representative from the Taiwan military. After the last event, RAND updated its adjudication of the wargame conducted in the first exercise to incorporate the selected technological solutions and assess their potential impacts. The ideas generated by the series of exercises are presented in the next chapter of this report.

Technological Solutions

Ultimately, our exercise participants generated a total of 17 distinct technological solutions that they believe could make a meaningful difference in the defense of Taiwan. We have grouped these solutions into six different categories based on their intended use and effect. We provide a summary of the discussion about each solution including the operational challenge it addresses, a short description of the solution itself, its development status, integration status, and potential operational uses.

Core Technical Infrastructure

Space/Ground Laser Communication

Operational Challenge

The PRC's electronic warfare capabilities have grown significantly in recent years. In an invasion of Taiwan, they could be employed to disrupt communication networks, impair joint maneuvers, and threaten the overall military effectiveness of U.S and Taiwan forces. New high altitude and space capabilities—which have proven their worth in Ukraine—could be used to maintain battlefield communications against an opponent with a sophisticated electronic warfare capability.

Potential Solution

Improvements to the communications platforms include multiple types of technological solutions. Satellites in multiple types of orbits – Proliferated LEO (PLEO), multi-orbit, MEO, or GEO – would provide many targets for the PRC to deal with. PLEO gives the most geometric diversity for node access and provides optimal latency and high bandwidth connections with highly manufacturable, low-cost, and existing technologies. Balloons or stratospheric ISR platforms would also provide significant value. Mesh networks would also improve the reliability and availability of communications. Using these capabilities in concert with each other would build in resiliency and redundancy for communications, expand the total amount of communications bandwidth available for battlefield C3, and complicate Chinese efforts to disrupt American and allied C3 through either electronic warfare or kinetic means.

Each of these new assets could potentially play multiple roles. While they would serve as communications nodes, they could also be used as Intelligence, Surveillance, and Reconnaissance (ISR) platforms, computational nodes, or platforms for electronic warfare or cyber operations.

The solution would also have these performance specifications:

- Robust communications within Taiwan and back to the United States.
- Improved communication speeds from Kbps to Gbps with less than 100 ms. latency.
- 10+ satellite per day output.

Development Status

The technology required for these communication mechanisms is mature, but not widely adopted. The current focus on higher orbits was conducive to a smaller number of exquisite systems. Moving these systems away from Low Earth Orbit makes them more likely to survive, but this comes with a trade-off: it reduces the ability to launch as many of them. These platforms, while fewer, would enable high-value assets and greater performing communications through larger form factor solutions. Systems like this exist today. Effort should be put into providing these assets an interface to the PLEO constellation as well as each other.

Rapid launch response capabilities can be used to augment constellations at short notice pre- or post-conflict. The technology exists and is mature, but it requires investment and acquisition by DoD.

Operational Impact

Improved space/ground communications could offer a reliable communications network which would be less vulnerable to enemy interference. Starlink's use in Ukraine has already proven the value of having new networking paths available for potential military use.

While this capability would be useful in any military context that requires the transmission of information, two operational use cases stand out. First, a reliable network would ensure that ISR assets are able to transmit their valuable intelligence back to the fires units who could act on it or to the headquarters units keeping track of the state of the battlefield. Second, reliable communications are essential to command and control of units throughout the theater. Both functions could meaningfully benefit from this solution.

Integrated Warfighter Network

Operational Challenge

Current communications are an incompatible mix of technologies and systems, typically designed to support a specific source/destination and a specific data type. An operational Integrated Warfighter Network (IWN) could break down these barriers to create a fully interoperable network that maximizes the ability to use any available link.

Potential Solution

The IWN would make use of multiple types of network connections to improve the reliability of communications. It would also improve military hardware so as not to be dependent on a

single type of networking connection but capable of flexibly using whatever connections are currently available.

Improvements to the network itself will be critical. Communications can be updated to use multicast protocols in order to minimize the impact on shared network paths. Traffic categorization and prioritization would also ensure that potentially scarce networking resources deliver the highest priority traffic. Networking components could be redesigned to “store and forward” messages and data when necessary, making the network tolerant of delays or occasional periods of a loss of connectivity.

Development Status

- While this solution will require engineering effort to implement, algorithms for computer networking have always been agnostic as to the specific transport path or transport paths used.

Integration Status

- Integrating the IWN into DoD’s existing equipment will be the primary issue. We will need to ensure that we do not introduce bugs or incompatibilities that reduce the functionality of existing equipment during any upgrade to support the IWN. While this need to ensure backwards compatibility will slow any transition to the IWN, it is not an insurmountable obstacle.
- Transport independence (the ability to use different transport layers for computer networking) is the primary aspect of IWN that has not yet been solved. While some equipment has been designed to be more network-agnostic than others, there are no solutions within DoD that can easily and reliably be reused across a wide variety of transport layers and types.

Operational Impact

The Integrated Warfighting Network ensures that individual pieces of military equipment or communications gear are able to use whatever network path might be available to them. This improved robustness increases both the likelihood that units or pieces of equipment have reliable communications and the amount of network bandwidth available.

This capability supports the same two use cases as the previous solution: connecting ISR assets to fires units and ensuring communications to enable command and control.

Edge Integration/Computing

Operational Challenge

Data fusion and analysis is vital for forward forces to create a comprehensive and accurate understanding of the operational environment. However, relying on inorganic computing

capabilities slows the process, and isolated or jammed units may be unable to exchange information for analysis.

Potential Solution

This solution would provide an edge computing¹³ capability to units at the brigade level and below. Providing an organic capability that allows these units to conduct real-time data processing near the source of data generation would enable rapid analysis and decision-making. Edge computing reduces response times by minimizing latency and allows for operation in environments with limited or unreliable connectivity, enhancing the autonomy and survivability of forces operating in or near contested zones.

This solution will provide the capability for computers attached to forward units to aggregate and analyze data that is received from sensors through multiple collection methods. Advances in context models and pretrained models can be used to assist in the identification of threats and provide target quality information and a common operating picture (COP) for local forces. Data could be shared vertically and laterally. In an invasion of Taiwan, forward operators could bring an “edge box” forward and connect it to sensors on organic Unmanned Aerial Vehicles (UAVs), local CCTV cameras, or other available sensors. The edge processor generates a COP that can be shared with allies and partners. The processor can also track targets and broadcast key sensor data. Users at the edge can exploit this information to speed their operations and identify targets. Critically, this capability should be simple to use and require minimal human input (e.g. only require a human for key decisions or to verify targets).

Development Status

Commercial firms currently employ technological solutions similar to this. There are some military-specific capabilities that could improve the utility of this capability in the context of this specific use case. These include:

- The networking component likely needs further development for military-specific scenarios.
- It is unclear exactly how many military tasks we can fully or partially automate. Iterative development with feedback from users will be necessary to understand what frontline personnel desire from the system in terms of modeling and output.
- To be effective, it needs to be transportable and have a minimum footprint. Eventually, the edge box might need to be the size of a PC.

¹³ Edge Computing refers to moving data storage and computation closer to the devices which produce the data and the users who consume it (the “edge” of the network) as opposed to bringing the data to a central data center and performing the computation there (as is more typical in cloud computing). AWS, “What is Edge Computing”, <https://aws.amazon.com/what-is/edge-computing/> as of November 19, 2023.

Integration Status

- Primary integration challenges involve data. Data standards would accelerate the integration of all the necessary components for this solution.
- Developers will need to make decisions about what data will be networked from organic sources and what needs to happen to make that data accessible.
- Multimodal support for many diverse sensor types is underdeveloped and integration testing would be necessary.

Operational Impact

The Defense Department already intends to field this technological solution and has well-developed requirements for it. However, it is not clear if there are plans to deploy this capability to Taiwan in advance of a conflict. If significant edge computing resources can be made adequately survivable, Taiwan forces would benefit from these capabilities just as American forces would. In particular, Taiwan would benefit from an ability to disperse its sensors and fires capabilities widely for survivability and to rely on networking to mass their effects when needed. This solution would also enable many of the other solutions discussed by the participants, such as improved Common Operating Pictures (COPs) or voice and text translation capabilities.

Command and Control

Joint Cross-domain COP

Operational Challenge

The United States and Taiwan lack the ability and classification authorities to view a shared picture of the battlespace. This limitation will inhibit their ability to share critical intelligence regarding force locations and status and targeting information in real time. Interoperable COP applications would allow for coordination to improve the effectiveness and efficiency of their operations.

Potential Solution

This capability would provide US and Taiwan forces a shared cross-domain COP. It would present a unified, real-time view of the battlespace, including the locations and status of friendly and enemy forces, as well as other relevant data. This shared understanding would facilitate efficient coordination and collaboration among different units, branches, and nations, enhancing operational effectiveness. The COP would support informed decision-making and combined forces targeting by providing accurate and up-to-date information, thereby reducing the risk of losses due to friendly fire, minimizing operational confusion, and enabling rapid, synchronized responses to changes in the battlespace.

Development Status

Demonstrations of solutions exist; there is no technological barrier. Acquisition policies complicate rapid development of a COP across services or with allies and partners, making the primary barrier one of policy. It would be necessary to consider data validation and procedural deconfliction across command and control systems as well as how to maintain operational security and manage information loads for system users.

Integration Status

Integration issues are primarily those of policy and culture, rather than technical issues. This capability could impact and disrupt the command cultures of the DoD and possibly Taiwan organizations. There are restrictive US policies around international classified data exchange, use of ‘dirty’ networks, and cross-domain systems. While these policies have a valid foundation, it will be necessary to consider the tradeoff between delivering information to warfighters in time to have an operational impact and keeping information secure from compromise. These are complex issues without any one-size-fits-all solution.

Operational Impact

This technological solution has the potential to meaningfully improve coordination at both the tactical and operational levels. At the operational level, it would primarily provide better decision support to senior leaders and ensure they are making choices based on all the potentially available information. At the tactical level, this capability would improve the coordination and effectiveness of fires and improve the integration of maneuver.

Document/Voice Translation

Operational Challenge

It is crucial for synchronization and efficiency in combined operations for allies and partners to communicate and collaborate. However, a basic language barrier and other practical barriers prevent US and Taiwan forces (as well as other potential allies and partners) from being able to communicate effectively and efficiently. This challenge manifests itself in two important ways. For one, language barriers inhibit U.S. and Taiwan personnel from studying each other’s doctrine and coordinating efforts prior to the onset of hostilities. Additionally, language barriers could also prevent effective real-time communication between US and Taiwan personnel at the tactical level during the conflict.

Potential Solution

This solution would involve two components. First, machine translation can be employed on written documents to facilitate a mutual understanding of core operational concepts. Both the

United States and Taiwan would collect releasable documents and multimedia relevant to their doctrine, CONOPs, and TTPs. Due to the scale of these data and the urgency of providing the information, they would be machine translated and shared with the relevant units to create a common understanding of each other's way of war. The archive should be readily available for reference to facilitate planning and operating to support the defense of Taiwan.

Second, facilitating communication between the United States and Taiwan is essential to enabling joint and combined operations and to providing US personnel (military and civilian) with the means to interact with their Taiwan counterparts as desired. The proposed solution involves creating a real-time method of translating spoken English/Taiwanese/Mandarin to enable communication. The application would run on equipment carried by deployed personnel and be air-gapped to enable operation regardless of connectivity. It would handle dialects of all relevant languages and accurately translate military jargon along with idioms.

Development Status

- Machine translation is a solved problem, although it generally requires the cloud or computing power in excess of what troops normally carry.
- Organizing the document archive and making it easily accessible is essential to making it useful.
- Air-gapped models need to be developed given the potential of interrupted internet access. The smaller we can make these models, the more devices they can be deployed to the field and the more end users can use them. The final product would be designed around the demands of these operational context and specific unit use cases.
- The language model needs to be able to handle idiomatic speech, military jargon, and dialects. Operational testing should be conducted in advance of the conflict to ensure the solution handles these use cases.

Integration Status

There should be limited integration challenges. Similar capabilities have been used in recent U.S. counter-terrorist and stability operations.

Operational Impact

This capability would benefit allied forces at both the tactical and operational level. At the tactical level, real-time voice translation would simplify communication between controllers on the ground (most often Taiwan forces) and allied pilots, sailors, or artillery personnel supporting with various types of fires. At the operational level, this technological solution would reduce the friction involved in coordinating across operations centers theater-wide and ensure a greater unity of effort. The overall impact of this solution should grow over time in a protracted conflict, as conditions on the ground increasingly deviate from pre-war plans and require a greater degree of ad-hoc improvisation and adaptation.

'Uncommon' Operating Picture

Operational Challenge

This solution reverses the typical requirements for a Common Operating Picture (COP). Normally, a COP is intended to represent as much of the collective real-time understanding of the battlefield environment among commands (or across allies) as possible, showcasing the location of friendly and enemy forces, current objectives, etc. However, the consequences can be severe if an adversary successfully penetrates this COP, as it can facilitate precise targeting operations and reveal the U.S. coalition's strategy in the conflict. If a cyberattacker were to steal this information, it could greatly facilitate an early defeat of Taiwan and American forces.

Potential Solution

The proposed solution represents the capability to share information with allies and partners using controlled methods that enable the coalition to execute a common plan without revealing the whole order of battle. This 'uncommon' operating picture with partners would obfuscate the exact location of U.S. coalitional forces, deliver spatially aggregated information, tailor information to certain geographic areas, and employ other methods to reduce the risk to the US and its allies if the PRC successfully accesses the system.

This process should be automated to be useful at the speed of war. So, the solution will adjust the fidelity of data based on a variety of factors. For example, a neighboring unit might be provided information about the portion of the unit closest to their position in order to ensure coordination between the units and prevent gaps, while higher-level headquarters might only be provided ISR information about enemy forces or information relevant to long-range fires. Before sharing, the system itself would consider both the utility of the data to the People's Liberation Army (PLA) in the event that it penetrates the COP and estimate the benefit to sharing the data with partners. As units move and objectives change, the 'Uncommon' Operating Picture would dynamically change what is shared across partners to reduce the danger to all friendly forces and their strategic aims. This model could filter each nation's contribution of information to the overall 'Uncommon' Operating Picture.

Development Status

There are significant developmental obstacles for this solution.

- As with any COP, integrating many different data sources across all levels of the military in real-time will be difficult.
- There is no existing model to predict the appropriate level of sharing given its characteristics. Likely requires a significant engineering effort to either train an AI/ML model or design an expert systems-based approach.

Integration Status

There are numerous integration challenges that focus on sourcing data.

- Integration of different data sources will be a significant challenge.
- There will be concerns regarding the ability to share sensitive intelligence data with partners and with the possibility that the enemy could gain access to the COP via a cyber hack or other means. The nature of the Uncommon Operating Picture in limiting the scope of potential enemy compromises should reduce these concerns compared to other command and control solutions (such as the Joint Cross-Domain COP solution above). However, the fundamental tradeoff between operational utility and information security will remain.
- If we choose to extend this solution to Taiwan's forces it will further slow development. However, Taiwan could also greatly benefit from this solution since they face the same challenges as DoD.
- Commanders – especially higher-level commanders - will fundamentally dislike the solution since it will give them a less complete operating picture instead of a more complete one. Many will likely want to know and potentially control the data that are being shared, rather than relying on a model to automate these decisions.

Operational Impact

In its fullest manifestation, this concept would modify the operation of every Common Operating Picture in use by American, Taiwan, or other forces. COPs that provide specifics about the location and condition of equipment or personnel would be particularly important to obscure. Similarly, incorporating these changes into COPs that support the activities of higher-level decision makers would also be more impactful compared to altering COPs that support tactical level units and personnel.

Blue-green Single System Aggregation

Operational Challenge

Effective coordination and information sharing between and within partner forces during war is pivotal to achieving strategic objectives, adaptive planning, and synchronized execution of operations. Disconnected systems, disparate data flows, and isolated computing environments limit the extent to which the US and Taiwan can coordinate through information sharing.

Potential Solution

This solution entails creating a ubiquitous computing architecture from senior command echelons down to the warfighter that uses a cloud infrastructure at each classification level (Unclassified, Secret, Top Secret). This architecture should be characterized by pervasive,

interconnected devices and systems that operate collaboratively to deliver on-demand services and information regardless of network connectivity.

By enabling this rapid, secure connectivity across forces and echelons of command, warfighters will retain access to information and tools critical to their operations. This architecture will greatly simplify data sharing between the US and Taiwan by providing standardized methods of exchange and a single aggregated system with which to interact. The system should be able to operate without connectivity and be offline for extended periods of time.

Development Status

- The technical pieces are developed. The only step left is to package and approve them.
- Partner forces require the right technology stack to integrate with this system.

Integration Status

Significant efforts are underway to integrate this sort of solution, but no entities appear to have a complete strategy or own the entire process. This integration is essential for its success. Multiple efforts need to be addressed to successfully integrate this solution:

- Scaling and sustaining the network and software-defined encryption
- Policy/security implementation
- Integrating legacy hardware
- Navigating the regulatory environment, especially DISA rules that increase the overhead of using cloud computing.
- Training of personnel across commands and nations.

Operational Impact

In the short term, this solution could most easily be fielded to support coordination across operational headquarters. Used optimally, it could improve the situational awareness of senior commanders, synchronize major operational movements, and streamline logistics. Using this solution to support tactical operations might require the creation of customized software to support specific use cases. However, events in Ukraine have demonstrated how creative tactical commanders can be in employing existing commercial software to support operational needs. If tactical units have assured communications allowing them to access cloud resources, their commanders could find great value in this solution as well.

Secure Mobile Devices

Operational Challenge

In modern warfare, static positions or equipment and personnel with highly visible signatures have extremely low life expectancies. Consequently, individuals and tactical commanders will

need a way to share information while remaining highly mobile and relatively concealed from detection.

Potential Solution

Potential solutions for mobile C3 include the following options:

- Direct to device communications¹⁴
- Mobile gateways (e.g. Integrated Warfighter Network, Starlink, etc.)
- Command phone and tablet experience but with appropriate classified data. Essentially, it is an extremely portable electronic device with the ability to change classification modes as necessary and to securely connect to SIPR and JWICS data. This device should provide the same user benefit at scale that modern commercial devices currently provide consumers (“it just works”).

Development Status

Commercial mobile devices in a variety of form factors (laptop, tablet, phone) are very mature. They have powerful computational hardware that is reliable and highly mobile. In the military context, unscalable and clunky devices deliver a partial solution to this problem, but they would not scale to support a Taiwan conflict. This solution requires less technical maturation but more policy flexibility to achieve.

Integration Status

The primary barrier to integration is cybersecurity processes. Once the devices are authorized, integration with voice communications and video/VTC is straightforward. Data integration with custom DoD software systems will not be as seamless, but it could be accomplished if the engineering effort is prioritized. The technical challenges in these integrations are conceptually straightforward and should not be difficult to overcome.

Operational Impact

This technological solution would ideally be available to essentially any servicemember who works with a computer today. The solution would improve command and control at all levels – tactical, operational, and strategic. The war in Ukraine has demonstrated the vulnerability of large headquarters detachments with correspondingly large emissions signatures and an inability to displace rapidly. This solution would help to ensure that these personnel could continue to serve their essential functions while remaining mobile and survivable.

¹⁴ Direct to Device communications (D2D) is defined as direct communication between two mobile devices without going through an intermediary

Intelligence Collection and Analysis

Situational Awareness Model

Operational Challenge

Leveraging a blend of sophisticated technology, traditional stealth techniques, and vast information controls, the Chinese military obfuscates its operations and activities. This makes it difficult for the US and its partners to accurately assess real-time military developments and strategic intentions. While preparing for an invasion of Taiwan, the PRC will employ hidden troop movements, covert development of weapons, and cyber operations camouflaged by a fog of disinformation and strategic feints to gain the initiative and strike when unexpected. It is therefore critical for the US and its partners to increase their situational awareness and to understand the PRC's decision-making processes and military intentions.

Potential Solution

The proposed solution represents the application of an advanced predictive algorithm, capable of utilizing multi-INT (intelligence) data. This algorithm would integrate and analyze a wide array of data inputs spanning social, political, economic, and military indicators updated in real-time to detect anomalies and patterns to ultimately predict PRC decision-making and behavior, possibly with human teaming. This solution could provide the US and its partners with added, actionable warning time in the event that the PRC decides to invade Taiwan.

The algorithm would be designed to continuously monitor and analyze diverse datasets, including satellite imagery (GEOINT), intercepted communications (SIGINT), open-source data (OSINT), human intelligence (HUMINT), and financial transactions (FININT). It would need to correlate increased military activity with these factors, relevant economic variables, social unrest, or changes in political leadership. Doing so effectively may require input from human analysts to help map those indicators onto specific predictions of PRC behavior. Ultimately, these algorithms would work alongside human analysts to simplify their job and enable the analysts to focus on the most promising intelligence by flagging anomalies and patterns among massive flows of data for humans to inspect.

Development Status

The discrete pieces of this solution exist, but creating a system that employs disparate pieces of data at scale to predict specific decision-making is novel and presents particular challenges.

- This solution requires extensive, cloud-based computational resources and an open architecture to ingest, curate, and manage data.
- LLMs can help detect anomalies in censorship, patterns, social media narratives, disinformation patterns, trade patterns, etc., but human analysts will need to map these phenomena to PRC decision-making.

- Much of this solution hinges on the curation of open-source data. Unfortunately, relatively little open-source data exists in DoD environments. It may be possible to leverage commercial software applications or data providers to acquire these types of data.
- Existing ML models may not be able to predict behavior they have not seen. Adapting to and understanding novel behaviors from the adversary will be challenging.

Integration Status

- Rhombus Guardian, Palantir, and commercial tools (e.g. OpenAI) may answer specific questions within this problem space, but integrating them is a challenge.
- Multiple different classification environments between the US, Taiwan, and other allies and partners could substantially hinder collaboration and information sharing.

Operational Impact

The existing state of technologies offers two paths for this solution. On one path, this model would predict strategic decision making in the PRC – whether Chinese leadership had decided to invade Taiwan, the likely timeframe for that invasion, which landing site had been chosen, etc. On the other path, this solution would instead focus on trend analysis. Using the technology in this way would provide indicators and warnings to US and Taiwan commanders when the situation was deviating from the norm and providing earlier warning of potential PRC actions.

This solution would have impacts both within the scope of our wargame exercise and outside of it. For example, if American leadership had earlier warning of a potential conflict over Taiwan and a greater confidence in those warnings, they could alter the force flow of units into the theater and they could rally allies around the globe to resist the invasion. This approach has paid significant dividends over the course of the conflict in Ukraine. Better knowledge of the enemy's plans as well as the status and locations of his forces could potentially allow decision makers in the United States and Taiwan to take earlier and more decisive steps in response, perhaps deterring Beijing from initiating hostilities. At the same time, invalid results could potentially set off false alarms or lead to bad decisions.

Identifying AI-Generated Adversarial Disinformation

Operational Challenge

Synthetic text and multimedia employed in adversary information operations during a PRC-Taiwan conflict pose significant operational challenges to coalition forces. They enable the adversary to rapidly develop and deploy information operations (IO) campaigns that spread false narratives, create confusion, and influence public opinion in their favor. The mobilization of Taiwan's reserves is a critical part of their defense and may be vulnerable to PRC information operations.

Potential Solution

The proposed solution represents the capability to employ deep learning algorithms to analyze and categorize vast volumes of digital information to identify disinformation generated by adversarial AI systems in order to preempt these operations. The solution requires collecting and analyzing data from the internet, including from social media, news websites, forums, and underground networks – in addition to more targeted monitoring of known sources of adversary IO campaigns, such as high-risk social media networks. Using natural language processing, image recognition, and computer vision, the capability identifies both text and multimedia content that may be a part of coordinated disinformation operations. By tracing the origin and spread of the disinformation, the coalition could respond to these campaigns by countering them with accurate information or by taking action against the source nodes disseminating the disinformation.

To achieve this, the algorithm uses digital forensics and network analysis to identify patterns, anomalies, and signature markers associated with commercial and adversarial AI systems at scale. Human-machine teaming may increase the system's utility and enable more agile adaptation to evolving conditions. The algorithm also maps out the propagation of the disinformation, revealing how the deceptive information is spreading and is expected to spread across networks.

Development Status

The pieces of this capability exist but scaling them together will present unique computational and practical problems. It will be challenging to deploy the model on classified environments. The team will need to ensure the PRC cannot manipulate this capability with data poisoning attacks or diversionary IO campaigns.

Integration Status

Services with similar architectures exist on classified systems, but the scale and integration with human analysts could pose challenges. Even after an effective AI model is trained, the product will need to be integrated into the workflows of intelligence analysts and analysts will need to be trained on how to interpret the outputs of the model. The full solution will also need to be connected to existing intelligence analyst platforms.

Operational Impact

Success in the information environment could be critical to the defense of Taiwan in several ways. First, success in this domain could have a meaningful impact on the 'will-to-fight' of Taiwan's reservist contingent and civilian population. Taiwan's active-duty personnel constitute only about 10% of its total military personnel; consequently, anything that would lessen the willingness of its reservist component to fiercely resist the invasion – or not show up

for duty in the first place – could have a catastrophic impact on Taiwan’s ability to defeat an invasion.

Additionally, success or failure in the information domain could significantly alter what kinds of assistance allies throughout the region are willing to provide American forces, for example, determining whether American aircraft can fly from friendly airbases or whether allied governments are willing to contribute their own forces to the conflict.

Unmanned Systems

Multidomain Drone Mimics

Operational Challenge

Intelligence, Surveillance, and Reconnaissance (ISR) would be vital for the PRC during an invasion of Taiwan. ISR would provide critical information on enemy movements, capabilities, and intentions and inform their offensive strategies and resource allocation. Successfully leveraging technology to deceive the PRC’s collection efforts would generate a meaningful operational advantage for the U.S. coalition.

Potential Solution

The proposed solution creates large numbers of multi-domain, multi-spectrum drones capable of confusing the enemy’s ISR. The key will be to ensure that these drones are both sufficiently low-cost and sufficiently convincing to confuse enemy targeting or draw enemy fire. Decoys could also play a key role in confusing the enemy’s strategic plan. The decoys could cause the PLA to incorrectly judge the dispersion of U.S. coalitional forces and may cause the PLA to choose the wrong landing areas or concentrate their forces against the wrong locations. As an extra benefit, the drones could also serve as nodes in a mesh network to help ensure robust communications or be equipped with an electronic warfare capability to disrupt the enemy’s operational picture.

One essential aspect of this solution will be that these drones should not require working in-theater runways for launch or recovery during the conflict. The PLA will attempt to render U.S. and allied bases across the theatre inoperative during the crucial early days of any conflict. Therefore, runway independence is essential in order for the joint force to be assured of being able to generate large numbers of air sorties at times and places of need. If these drones do require working in-theater runways, it will limit their utility during the crucial early phases of a conflict.

Development Status

A wide range of Unmanned Aircraft Systems (UAS) with payloads that are useful for deception have been fielded for military and commercial uses. The primary question is the

purpose for which the system is being developed. For example, small UAS could be deployed to Taiwan to act as emitter decoys for radars and radios while medium UAS could deploy between dispersed airfields on Japan to simulate aircraft and large UAS could simulate aircraft flying around the theater.

Care will need to be taken in developing systems that will successfully deceive while minimizing their cost. In some cases, it may be possible to simply hide signal in large amounts of noise, but in others, systems will need to fool sophisticated ISR capabilities. While creating inexpensive and numerous decoys would be ideal, it will ultimately be more important for these decoys to create a convincing deception than it will be to field them in overwhelming numbers.

Successfully mimicking 5th generation fighter aircraft will also likely require decoys to fly at high subsonic speeds. To do so, the decoys would likely require substantial engine thrust to achieve with corresponding increases in the size, weight, and cost of the decoys.

Operational Impact

The highest impact operational use case for this concept varies depending on the expected timeframe for the conflict. If allied planners assume the conflict will only last for a short duration, the highest impact use for decoys would be to create mimics of 5th generation fighter aircraft. These types of decoys would confront enemy fighter patrols with a multitude of phantom signatures to chase, absorb enemy anti-air missiles, reduce the loiter-time for enemy combat air patrols, and confuse enemy commanders as to the timing of when American fighter patrols would be arriving over Taiwan and in what strength. They could also be used to confuse which airfields are operating and at what times.

If we believe that the conflict over Taiwan will instead become a protracted affair, the value of decoys which mimic large body aircraft (air refuelers, airborne early warning aircraft, and heavy bombers) increases. In a quick war, the most likely rates of attrition for these platforms would not be sufficient to meaningfully affect the course of events. However, over an extended duration, the shrinking number of available aircraft and lengthy time period required to replace losses could begin to have a meaningful impact on the United States's ability to support combat operations in the theater. For our wargame scenario, we ended our simulation after a relatively short conflict duration (1-2 days of pre-invasion bombardment followed by 7 days of ground combat on Taiwan); consequently, our evaluation primarily focused on considering the impact of decoys of 5th generation fighters. This does not mean that other uses for multi-domain mimics would not have merit; several potential uses of this technological solution could prove useful depending on what baseline assumptions are made about the nature of the conflict over Taiwan.

Advanced Mines

Operational Challenge

Mines have long been an essential part of countering a potential invasion. However, static minefields are vulnerable to enemy minesweeping and it will be difficult for Taiwan naval forces to extend or replenish these minefields after the onset of hostilities.

Potential Solution

The proposed solution represents the capability to deploy AI/ML enabled maritime mines that can reposition themselves and swarm targets. They could be used to destroy high-value targets or to channel PLA naval forces towards kill boxes sown with dumb mines. These minefields could help allied forces secure the Strait and limit the PLA's amphibious assault of Taiwan.

The AI/ML-enabled mines could be deployed from UUVs or self-deploy from ports or other appropriate access points. Mines would use multiple information sources and a heuristic algorithm to communicate with one another relying on temperature, pressure, and the electromagnetic spectrum. Selectively concealing the extent of the network and the location of the mines from the PLA is essential.

Development Status

Non-AI smart mines exist, but collaborative and swarming behaviors have not yet been developed to enable this capability.

- Ideally, the model needs to understand and predict PLA movement, coordinate with U.S. coalitional forces, and interdict targets in a manner consistent with the operational commander's overall plan.
- Different operational use cases have different degrees of complexity. For example, detecting and tracking a massive invasion fleet is substantially easier than deciding if an individual ship is a PLA minesweeper or a neutral freighter.

Integration Status

Smart mine development and integration is underway, although not with these capabilities.

Operational Impact

In the near term, we assume that only a few hundred of these improved smart mines could be produced. Given this assumption, smart mines would most likely prove most effective for three purposes. First, smart mines could position themselves to disrupt the PLA invasion force just prior to its assault on the beachhead. Any physical losses incurred by the invasion fleet would be magnified by the psychological impact of the attack on inexperienced vessel crews and by the limited ability of the Chinese military to improvise and adapt to deviations from pre-planned operations. Second, some smart mines could be kept in reserve to deny Chinese forces

the ability to use captured Taiwan port facilities. Even if only a few smart mines are available for this purpose, a plausible threat supplemented with decoys could deter Chinese forces from risking vulnerable logistics assets and divert Chinese military power. Finally, a viable threat from smart mines could force the diversion of Chinese minesweeping assets to protect the invasion force while in harbor or sweep the Chinese inland waterways which provide an essential logistics capability for Chinese forces. While the majority of smart mines should not be employed near the Chinese mainland, a handful of attacks would present a threat that might require a disproportionate diversion of Chinese resources to counter.

Short-range strike UAVs

Operational Challenge

Slowing the PRC's amphibious assault and preventing it from establishing a beachhead during the invasion is vitally important. Technology can help the US target the PLA invasion force during this critical period.

Potential Solution

This solution would involve prepositioning short-range strike UAVs (akin to Switchblade drones) on Taiwan. Prior to the invasion, they would be packed in containers and stored at strategic locations for deployment during an invasion. While resupply of these drones during the conflict would most likely prove impossible, they could easily be shipped to Taiwan ahead of the conflict. The priority for these UAVs would be to protect beachheads, landing zones, and chokepoints.

These UAVs could be designed with a high degree of autonomy if intended for use in areas where only hostile targets are likely to be present. For example, it is unlikely that friendly or neutral ships or helicopters would be present near PLA landing zones or invasion routes, potentially simplifying the training of computer vision algorithms to automatically target hostile forces. Restricting the use of these munitions only to geographic areas where civilians and non-combatants are unlikely to be present may alleviate concerns about allowing for their increased use of autonomy.

Development Status

Commercial efforts and demonstrations currently exist. There are also active military concepts.

- There are manufacturing needs to build out these capabilities.
- Autonomy in this context needs further development.

Integration Status

Depending on the exact requirements, there are limited integration challenges given existing programs that use UAVs. A primary challenge is willingness to allow autonomous systems to actively engage near populated areas with minimum human input.

Operational Impact

These strike UAVs could have multiple operational use cases. In our simulation, one of the most valuable uses of these UAVs would be to target PLA helicopters during an air assault. Large numbers of relatively low-cost drones similar to existing capabilities such as the Switchblade would threaten to inflict massive casualties on any such attempt. The mere existence of such a capability might well deter the PLA commander from attempting such an operation. Drones could also target troops exiting amphibious landing craft or vehicles on the beachhead.

Medium-range ISR UAVs

Operational Challenge

Maintaining persistent ISR coverage both pre- and post- invasion will be essential to maintaining situational awareness and countering Chinese activities.

Description of Solution

This solution would involve prepositioning low-cost, medium-range UAVs on Taiwan as well as rapidly converting civilian and hobbyist UAVs during a pre-invasion warning period. Prior to use, these drones would be packed in shipping containers that are mobile and low-profile. Taiwan forces would be expected to lose large numbers of these types of drones; for context, Ukrainian forces have lost approximately 10,000 drones per month during their conflict with Russia¹⁵.

Establishing a standard communications and sensor package for these drones could allow for the rapid conversion of civilian and hobbyist drones during a pre-conflict warning period. The drones could be linked through a mesh network to improve the reliability and robustness of communications. They could also carry a standard sensor package which could be upgraded over time. Initially, these drones would likely carry cameras enhanced with computer vision algorithms, to locate and identify hostile vessels in the Taiwan Strait or track the Chinese invasion force after it has come ashore. Although these aircraft might not be able to provide sufficiently detailed information for targeting purposes, they could greatly improve Taiwanese ground targeting. Ukrainian forces have leveraged UAVs with similar capabilities to

¹⁵ RUSI, *Meatgrinder : Russian Tactics in the Second Year of its Invasion of Ukraine*, May 19, 2023.

substantially improve their ability to detect enemy forces and rapidly provide corrections to fires units targeting them. Importantly, these UAVs would not require runways for launch or recovery and would continue to operate even if Chinese bombardments render airbases on Taiwan unusable. However, they would still require functioning energy sources.¹⁶

Development Status

Commercial efforts and demonstrations currently exist. There are also active military concepts.

- There are manufacturing needs to build out these capabilities. Right now, China is the world's UAV factory.
- Primarily will require investment in building the software for the mesh network.

Integration Status

The primary integration issue concerns data integration. The data collection must be transmitted and processed somewhere while under heavy communication degradation and vehicle destruction. Commercial UAVs would also likely need to host software providing them with some degree of compatibility with military systems if integrated command, control, and intelligence collection is needed.

Operational Impact

The primary operational advantage for this solution would come from deploying the UAVs over the Taiwan Strait to detect the PLA invasion fleet and help predict its most likely destination. Many low- and medium-cost UAVs possess the necessary range and payload to operate over the Taiwan Strait. With sufficient early warning of Chinese intentions, civilian UAVs could receive a software update to support a standard sensor and communications package before being shipped to Taiwan en masse. Cheap UAVs could also clutter the Chinese radar picture, allowing more capable drone aircraft with electronic warfare or even strike missions to hide among a swarm of less capable vehicles. While the limited payload capacity of these drones might prevent them from carrying sensor and communications packages capable of relaying information precise enough for targeting purposes, they would provide continuous coverage over the route of any invasion fleet.

¹⁶ For an assessment of the potential for autonomous UAS to provide persistent ISR and targeting in future conflicts, see Thomas Hamilton and David Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environment: Preliminary Evaluation of Operational Concepts*, RAND, RR-4407-AF, 2020.

Applications to Improve Training

Commercial Combat Suite

Operational Challenge

Minimally trained reserve and non-military elements can serve a crucial role during war by providing additional manpower and specialist capabilities that supplement active-duty military personnel. How can Taiwan use technology to train, prepare, and integrate these elements? How can it provide them an accessible process that facilitates combat operations tasks?

Potential Solution

This solution would provide a suite of software applications based on three principles. First, it would maximize the use of commercial software technologies with an established market share in Taiwan. For example, soldiers in the Ukrainian military have frequently relied upon commercial software applications such as Telegram, Signal, and WhatsApp for command, control, and communications on the battlefield. Similarly, there are many commercial software applications that help manage business work processes which would be familiar to much of the private sector workforce and could potentially be adapted to military workflows. By using existing software applications which Taiwan users are already familiar with, this solution eliminates acquisition risk and useability risk.

Second, this solution would include a training and simulation component so Taiwan reservists can complete many repetitions of the most critical workflows. Ukrainian units were able to perfect their “commercial combat suite” during an extended period of warfare following the Russian invasion of 2014. This capability had reached a very mature level by the time of the 2022 invasion and provided substantial benefits to Ukrainian forces. While an artificial training environment cannot fully replicate actual battlefield experience, more realistic training that is frequently repeated could substantially boost the performance of Taiwan reservist units. Ideally, this would include a “gamified” component to its training. If training was both fun and realistic, it could encourage many Taiwan reservists to train even when not required – simply because it is enjoyable. In the best-case scenario, virtual training might acquire the popularity of an e-sports league, spurring voluntary engagement with a significant portion of Taiwan’s population and generating a no-cost expansion of Taiwan military training activity. Even better, tournaments could identify units with especially high levels of competence and cohesion. All of these aspects could improve the basic competence of Taiwan reservist units, increase unit cohesion, and improve the average will-to-fight of Taiwan forces.

Finally, some software applications within the Commercial Combat Suite could be created to optimize tasks deemed especially critical to resisting or preventing a Chinese invasion. For example, Ukrainian forces learned from their ongoing combat against Russian forces since 2014 that they needed to build some custom applications for intelligence integration and fires

solutions. These applications cannot simply be copied – the Taiwan scenario will be substantially different from that in Ukraine – but there will be equivalently critical tasks for the Taiwan military which could be optimized with purpose-built software. Integration of sensor data and fires coordination are two likely candidates, but the Taiwan military should learn from the Ukrainian experience to identify their own priorities.

Developing applications intended for use by a significant portion of Taiwan's population does likely mean that these apps will be accessible to the PRC, either through active sympathizers or by cyber compromises of unwary users. However, these risks can be minimized. The training applications would be the most vulnerable to enemy compromise, however compromising this component would also yield the least value since the enemy would only be able to observe Taiwan citizens repetitively learning relatively basic military skills and this part of the suite would have no role in coordinating operations once the fighting started. Commercial communications applications such as Line, WhatsApp, and Signal each have private, invitation-only group chats which could easily be used to create a cellular communications structure for the Taiwan military. Enemy agents would have to be serving members of the Taiwan military and would only have access to a relatively small number of relevant communications channels. Any agent would also have to transmit the information they learned to the PRC during wartime – most likely while the PRC was attempting to cut off Taiwan's communications with the rest of the world. Finally, Taiwan would have to ensure that enemy agents did not contaminate any custom-built software applications with erroneous information. Ukraine's experience developing and utilizing these types of applications demonstrates that they can be designed to be resilient in the face of enemy disinformation and manipulation; however, it will be essential that any such applications are designed to be robust even when enemy agents have the ability to send erroneous reports as input.

Development Status

There is a straightforward path to development and fielding. It primarily relies on existing fielded commercial technology with high user adoption among the Taiwan population.

- Could potentially adapt an existing massive, online multiplayer game or contract with an established computing gaming company to create the training component.
- Effectiveness depends on user engagement.
- Relies upon resilient network infrastructure in Taiwan but does not require connectivity between the island and the rest of the world. Leveraging existing commercial software applications may improve resiliency against Chinese cyber-attacks, since these applications are often supported by top-tier private sector cybersecurity teams and have a track record of resisting cyberattacks from a variety of malicious actors.

Integration Status

- Commercial messaging/communications apps only require a willingness to use. May face institutional resistance since they are not on ‘secure’ networks.
- Requires cooperation (or at least tolerance) from commercial entities that may not view themselves as being defense contractors or involved in a war over Taiwan. At the same time, this solution does not require commercial companies to donate their services or otherwise change their typical organizational routines – they are merely being asked to continue supporting their products for their customers.

Operational Impact

This solution would improve the effectiveness of Taiwan forces in three ways. First, this solution would arm Taiwan forces with a reliable and robust communications layer to improve command, control, and coordination on the battlefield. Taiwan’s use of these capabilities would mirror the experience of Ukrainians forces who have often relied upon widely available mobile phone applications as their primary way to coordinate operations and connect sensors with shooters. Second, this solution would ingrain essential behaviors and routines into Taiwan military personnel to better prepare them for the shock of combat. Finally, it would improve unit cohesion and will-to-fight by giving Taiwan units the opportunity to frequently work together at practical tasks and to engage in friendly competitions against other units. All of these factors would be especially impactful on Taiwan reservist forces and on active-duty forces with no prior combat experience.

Optimize Decoy Deployment and Deception Employment

Operational Challenge

Strategic deception during war can manipulate an adversary's understanding of reality, thereby creating opportunities to achieve an advantage. Misdirecting or delaying the PRC would be critical during a conflict to preserve weapons and supplies and to generate openings for offensive operations. Leveraging technology to inform the optimal way to employ deceiving techniques, such as decoys, feints, misinformation, or camouflage, during a war with the PRC could yield substantial benefits.

Potential Solution

There is currently no guide that advises when it is useful to use deception and survivability techniques. This solution would provide a software application that assesses whether deception is likely to be effective to meet specified objectives and, if so, the optimal type and quantity to deploy. It would incorporate information from a COP and known satellite orbits to identify possible adversary platforms that would be collecting on a unit. It could inform the use of force maneuvers, camouflage, physical decoys, electronic decoys, cyber decoys, and information

operations to deceive the PRC. As the effectiveness of a recommended technique decreases, it can alert users of a more optimal deception technique or that broader adaptation may be necessary. In a defense of Taiwan, it could be used for applications such as airbase defense by informing when to move or deploy real and decoy aircraft, fuel trucks, munitions, etc.

Development Status

This solution involves many different technologies with different levels of development.

- Aspects for individual deception exist, but there has been minimal work on combined optimization.
- Requires multiple sources of friendly and enemy data to gauge effectiveness. These data cross classification levels and will require access to commercial data as well.
- Full implementation will have a high logistics demand (for improved materials to construct better decoys). However, a simple version for when to hide, scatter, move, or cease emissions would only require data feeds.
- Our participants knew of no existing work towards an inclusive program like this that works across techniques, despite some movement on integrating models for individual techniques.

Operational Impact

Improved camouflage, concealment, and deception techniques (CCD) could prove beneficial across a wide range of operational contexts. CCD could prevent the PLA from locating and eliminating high value assets on Taiwan such as Patriot missile batteries or artillery weapons during the pre-invasion bombardment. This would expand the amount of firepower available to attack the invasion beachhead while Chinese forces are at their most vulnerable. Improved information about the enemy's ISR threats and how to best deceive them could prove especially useful to inexperienced Taiwan reservist forces.

In addition to improving their CCD techniques, American and allied personnel stationed outside of Taiwan could leverage this information to alter the view Chinese ISR assets have of their operational procedures. Deceiving PLA forces about the size, composition, and location of military forces supporting Taiwan throughout the theater could inject uncertainty into the plans of PLA commanders and trick them into focusing on the wrong threats.

Logistics

Predictive and Prescriptive Logistics

Operational Challenge

Efficient logistics is paramount to sustaining combat operations and enabling quick responses to changing battlefield conditions. Failure to provide adequate materiel and supplies at the right time and in the right place can severely hamper operational effectiveness.

Potential Solution

This solution creates a logistics data mesh that forecasts needs and optimizes supply chain operations during war. It requires the interoperability of all relevant data (for example, historical information and operational parameters) and logistics systems. It would track, analyze, and predict requirements across all commodities at all classification levels across all echelons. The proposed solution would work across the levels of war:

- Strategic: Perform readiness assessments across units and prioritize pushing materiel based on current and forecasted needs.
- Operational: Balance readiness across the areas of operations and automate delivery systems (e.g. UAVs). ‘Owners’ are the services and ‘users’ are everyone, including Taiwan military.
- Tactical: Use ML to generate predictions of where attention and maintenance are needed.

Importantly, this solution would allow U.S. and partner militaries to more efficiently move to a “push” logistics approach instead of a “pull” approach. The advantage is that a push system minimizes communications traffic and should increase the survivability of unit headquarters and command staff. The disadvantage is that this might increase the need for movement and transport. However, this will be reduced as the system becomes more precise and effective.

Development Status

Individual logistic systems are mature but often siloed. The solution requires integrating and resolving multiple technologies.

- Predictive analytics is mature. Optimization is the focus here.
- Data readiness, cleaning, and mapping will all take meaningful effort.
- There remain questions about universal standards/compatibility/interoperability.
- There are concerns about data governance and protection.

Integration Status

There are clear obstacles with data integration and DoD culture.

- Solution runs counter to DoD bureaucracy.
- DoD logistics systems frequently are not interoperable and often lack features commonly found in commercial logistics software (APIs, microservices, etc.).
- Title 10/50 data walls inhibit data interoperability and accessibility.

Operational Impact

This technological solution would probably have the greatest impact on a protracted conflict. In the first few days of the conflict, the primary logistics decisions will be when to stop flowing materiel due to the intended recipient no longer being sufficiently combat effective to require it. In the short term, logistical constraints will probably have a minimal impact on operations; however, as greater amounts of weapons and other materiel are expended, logistical concerns will loom ever larger. Moving to a push logistics system would improve the survivability of tactical headquarters, since it would minimize their need to transmit their logistical needs as part of a pull logistics system. If predictive algorithms are also able to improve the dispersion of limited resources, it would also help to ensure that units are able to both stay in the fight longer and operate with a greater overall combat potential. This would also improve the efficiency of employment of air and ground delivered long range munitions.

Analysis of the Impact of the Technological Solutions

Assumptions for Evaluation

One mechanism RAND leveraged to analyze the potential impact of these technological solutions was wargaming. The first exercise in our series established a baseline scenario modeling how the United States and Taiwan might defend against a Chinese invasion. RAND analysts took the record of gameplay from this exercise and updated the models evaluating combat actions and other outcomes within the game to incorporate the estimated effects of specific implementations of the technological solutions generated by our participants. For simulation purposes, we assumed that each technological solution received at most 20 million dollars in funding during the pre-conflict period (from 2023-2027) and up to 100 million additional dollars if the solution could rapidly be scaled up after preparations for an invasion had been detected (we assume clear indicators and warnings of an invasion would be detected at least 3 months prior to the onset of hostilities). The solutions proposed were very broad and had few of the details needed to estimate their effects in a scenario, therefore considerable expert judgment was used to choose specific numbers, locations, and employment concepts, as well as their effects. The concepts were assumed to work as envisioned, and enemy operations were not changed in response. Therefore, the results provided should be seen as high-level estimates based largely on expert judgment and could vary widely given different assumptions.

Our wargame scenario only lasted for the first week of what could be an extended conflict. In this scenario, Chinese forces bombarded the island for two days prior to launching a combined amphibious and air mobile assault and the game play ended five days after the initial Chinese landing with Chinese forces still advancing inland. Consequently, some technological solutions had relatively little impact on the course of events within the elapsed time. For example, we did not analyze predictive logistics because we expect that logistics and resupply would not be a significant problem during the first five days of a conflict. However, if we had analyzed a more protracted conflict, this solution could have been much more impactful. Similarly, some technological solutions had impacts that are outside of the scope of the wargame. The *Identifying AI-Generated Adversarial Disinformation* solution is one example of this. While success or failure in the information environment could have a substantial impact on any conflict over Taiwan (potentially changing the willingness of allies to assist a US-led coalition or changing the will-to-fight of Taiwan reservists), these effects largely impact the assumed starting state for the game. In order to fairly evaluate the impacts of our technological solutions that affected events within the scope of our simulation, we did not change the assumed starting conditions of the wargame simulation; however, solutions with impacts outside the scope of our wargame could still make a significant contribution to defeating a Chinese invasion of Taiwan.

Evaluative Approach

RAND has an extensive suite of tools to support wargaming. The most recent collection is R-FLEX (RAND Framework for Live Exercises, a system for adjudicating live wargames) which has rulesets that are flexible to data inputs¹⁷. Air and maritime combat use operational models that use aggregated data from engagement models. Ground combat uses a spreadsheet model derived from the R-FLEX game rules.

For air combat, a series of exchange ratios and kill capacity limits are applied at a force-on-force level assuming a specific strategy for each side. Exchange ratios and kill capacities for this wargame are calculated in the commercial version of the U.S. military's TACBRAWLER air combat modeling system¹⁸. All exchange rates and kill capacities are by generic aircraft generations versus by specific aircraft types. For overall strategies, the PLA is assumed to focus on denying the U.S. air superiority and the U.S. is assumed to focus on attacking PLA high value aircraft and supporting periodic strikes by U.S. bombers. The model also accounts for the rate and ability of aircraft to launch sorties from bases under attack and incorporates sortie rates from RAND's Combat Operations in Denied Environments (CODE) suite of models¹⁹. The unclassified version used in this wargame is a "light" version in that it only accounts for variables with available data. In this case, air-to-air munition inventories for the PLA are untracked and assumed as unlimited. Capacity of aircraft to support strikes and counter rotary-wing aircraft is also tracked. The methodology has previously been verified against more complex campaign results.

A driver of aircraft performance improvement was due to improved ground decoys and CCD measures that improved ground survivability and resulting sortie rates. An additional driver was the greater system integration for domain awareness that increased the coordination of fires rules for improved exchange ratios.

Maritime combat is divided into a submarine warfare component and a surface warfare component. The submarine warfare model evaluates submarines by category and generation for their ability to search, detect, engage, kill, and survive. Surface ships, uncrewed systems, and maritime patrol aircraft are also accounted for by generation and formation. All results are compiled as binomial distributions that are adjusted via a series of factors to account for specific environments and technologies and are modular to account for sensitivity of data. Mine warfare

¹⁷ Yuna Wong, Sebastian Bae, Elizabeth Bartels, and Benjamin Smith, *Next-Generation Wargaming for the U.S. Marine Corps*, RAND, 2019.

¹⁸ R. M. Kerchner et al., *The TAC Brawler Air Combat Simulation Analyst Manual*, rev. 3.0, Decision Science Applications Report No. 668, 1985.

¹⁹ Brent Thomas, Mahyar Amouzegar, et al, *Project Air Force Modeling Capabilities for Support of Combat Operations in Denied Environments*, RAND, 2015.

is included in this model. The methodology has been extensively validated against U.S. Navy modeling and simulations.

The surface warfare component focuses on missile interactions with surface platforms. All engagements follow strict engagement sequences accounting for early warning, aircraft, datalinks, radars, missiles, non-missile defenses, electronic warfare, and related tactics. Missiles are tracked via salvos whereas ships, ship radars, and concurrent engagement capacities are individually tracked. The model and results have been validated against engineering models, U.S. Navy operational models, and real-world test data. An unclassified only dataset treating all capabilities as equal by generation and type was employed.

Improvements in maritime performance resulted from an increased density of mines, improved timing supporting a higher percentage of missiles entering within acceptable area of uncertainties for seekers, and fewer PLA maritime patrol aircraft due to an improved air battle.

Ground combat modeling is based on brigade combat scores summed from equipment scores drawn from the JICM campaign model and based on expert judgment. Combat results were derived from commonly accepted rules-of-thumb given combat score ratios and the situation on the ground. The effectiveness of and losses to aircraft and helicopters were derived from estimates of the number of engagements and system effectiveness.

Ground combat improvements arose from improved coordination and CCD measures for Taiwanese ground forces to have improved survivability, improved coordination for better timeliness of fires and targeting ashore, and small unmanned munition densities of sufficient range and mass to attrite rotary-wing aircraft. Lessons learned from Ukraine were a consideration.

Major Impacts of the Technological Solutions

Ultimately, these new technological capabilities resulted in three major impacts on the conflict. To begin with, the synergistic employment of two solutions (*Multi-Domain Drone Mimics* and *Optimized Decoy and Deception Employment*) has the potential to substantially reduce the losses of American fighter aircraft especially at airfields. Our analysis concludes that these solutions could reduce the loss of 5th generation fighter aircraft by as much as half during the first five days of the conflict (over one hundred US 5th generation fighters were destroyed in the unmodified wargame). The resulting increase in available US fighter strength causes Chinese fighter losses to increase by approximately 70% within the first five days of hostilities.

Additionally, the technological solutions reduced the Chinese amphibious forces which are able to land on Taiwan. In the original wargame scenario, half of the Chinese amphibious forces (36 of 72 PLA battalions) survived Taiwan and American attacks to land on the beachheads. Assumed improvements from the technological solutions in smart mines, situational awareness,

targeting of munitions, and utilization of unmanned systems could reduce the number of amphibious battalions landed on Taiwan to approximately one-third of the force. The collective capabilities allowed munitions to be delivered in a timely, coordinated manner to the right beaches as opposed to directly improving individual munition performance. While we did not analyze the cumulative intangible impacts of these losses on the cohesion and will-to-fight of the Chinese force, no amphibious landing in history has ever sustained losses of this scale and ultimately emerged victorious.

Finally, the technological solutions reduced the Chinese air-assault forces which are able to reach Taiwan. In our assumed implementation of the technological solutions, Taiwan reservist brigades can guide small, loitering munitions against the helicopter assault force. We estimated these munitions could kill as many as one hundred helicopters in the first five days, or nearly one-tenth of the helicopters allocated to the invasion and as much as an additional one-tenth of their air assault force compared to the original game. If this capability was scaled up or was effective against the first waves of air mobile forces, it could potentially relegate air mobile forces to resupplying established beachheads.

The technological solutions that were set out above were assessed to have the potential to make a significant difference in our scenario covering the first five days of an invasion. The effectiveness of the solutions of course depends on many factors, including how these broad technology descriptions are implemented and employed and how Chinese forces react to the deployment of these capabilities, and even significant increases in Chinese losses may not lead to the defeat of the invasion without further reform and improvement in Taiwan's forces.

Conclusions and Recommendations

Ultimately, this exercise series proved useful for two reasons. At the tactical level, the series exposed private sector technologists to the key problems and difficulties the United States and its allies would face in defending Taiwan against Chinese aggression and enabled them to collaboratively develop practical new innovations to potentially overcome these difficulties. At the strategic level, the events demonstrated how to forge closer relationships between the Defense Department and America's vibrant private sector. As the 2022 National Defense Strategy relays, leveraging America's enduring strength in private sector led innovation is the key to preserving America's strength and deterring future aggression by America's adversaries. Based on our experience facilitating these exercises and analyzing the solutions they generated, we draw the following three policy conclusions.

- First, the Defense Department should engage in more immersive outreach efforts to innovators in the private sector to better contextualize military operations. During the events, many of the technologist participants remarked at how useful it was for them to be able to directly engage with DoD personnel to hear more about exactly what their problems and difficulties are and how rarely they had an opportunity to do so. This also correlates with best practices for innovation established by the technology sector.²⁰ The most effective technological solutions and innovations in the private sector do not come from simply handing an engineering team a pre-determined set of requirements and ordering the team to build that solution. Instead, the best technological solutions are developed when technologists have the opportunity to deeply understand the problem they need to solve from the perspective of the end user and then iteratively develop a solution while receiving constant feedback about their early prototypes. If the Defense Department wants to effectively leverage America's enduring capacity for innovation, it needs to adjust both how it engages with the private sector and how frequently it engages with the private sector.
- Second, this exercise series demonstrated that technological solutions exist which could both be deployed to warfighters at scale in the short term (next 3-5 years) with minimal technological risk and which could meaningfully enhance America's ability to defend against Chinese aggression in the Indo-Pacific theater. We do not claim that our list of technological solutions is either optimal or exhaustive – America's innovators have always been full of good ideas. However, this experience demonstrates how tapping private sector innovation can be put into action.
- Third, several technological solutions demonstrated the potential to have a game-changing impact on a potential conflict over Taiwan. The advanced mines solution drew the greatest interest from our 'Shark Tank' panel. Smarter mines incorporating advanced

²⁰ Marty Cagan, *Inspired: How to Create Tech Products Customers Love*, John Wiley & Sons, 2017, p. 29; Eric Ries, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, Crown Business, 2011.

algorithms would be extremely difficult to neutralize and could easily inflict chaos on the precise choreography necessary for any major amphibious invasion to succeed. Similarly, sufficient quantities of cheap loitering munitions could turn any attempted airborne or air assault by PLA forces into a suicide mission. In the face of such a capability, PLA commanders might well be deterred from even attempting such a risky operation. Just as importantly, in our wargame, most losses of American fighter aircraft occurred on the ground from attacks by Chinese ballistic missiles. Optimizing effective decoy and deception techniques (including the ability to understand and react to a dynamic ISR environment) could substantially reduce losses of advanced fighter aircraft and enable the United States to achieve air dominance earlier in the campaign compared to the status quo.

While these three technologies achieved the most direct impacts on warfighting outcomes based on RAND's analysis, it is important to remember that technological solutions with less quantifiable effects can prove to be just as important. Starlink's critical role in enabling Ukrainian military operations demonstrates the direct tie between improved communications and networking and battlefield success; American forces are even more reliant on these capabilities compared to the Ukrainian military. Nearly every commander in the armed forces wishes he or she had a more comprehensive Common Operating Picture to improve command and control. Finally, improving the proficiency and will-to-fight of Taiwan's sizable but inexperienced reservist forces could dramatically alter the balance of forces on the island. All of these potentially game-changing solutions are based on mature technologies and require relatively little investment to build. Although building out any of these ideas from the initial concept into a finished product would require additional analysis and iterative development to perfect, they each have the potential to meaningfully assist American and allied warfighters in defeating their future adversaries.

Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
C2	Command and Control
C3	Command, Control, and Communications
CCD	Camouflage, Concealment, and Deception
COP	Common Operating Picture
DISA	Defense Information Systems Agency
DoD	Department of Defense
EW	Electronic Warfare
HPC	High Performance Computing
IO	Information Operations
ISR	Intelligence, Surveillance, and Reconnaissance
IWN	Integrated Warfighter Network
JWICS	Joint Worldwide Intelligence Communications System
LEO	Low Earth Orbit
LLM	Large Language Model
MoD	Ministry of Defense
ML	Machine Learning
PLA	People's Liberation Army
PLEO	Polar Low Earth Orbit
PRC	People's Republic of China
SIPRNet	Secret Internet Protocol Router Network
UAV/UAS	Unmanned Aerial Vehicle / Unmanned Aircraft Systems
UUV	Unmanned Underwater Vehicle
VTC	Video Teleconference

References

- Cagan, Marty, *Inspired: How to Create Tech Products Customers Love*, John Wiley & Sons, 2017.
- CNAS, *Dangerous Straits: Wargaming a Future Conflict over Taiwan*, June 15, 2022
- CSIS, *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan*, January 9, 2023.
- DoD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 2018
- DoD, *2022 National Defense Strategy of the United States of America : Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review*, October 27, 2022.
- Hamilton, Thomas and David Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environment: Preliminary Evaluation of Operational Concepts*, RAND, RR-4407-AF, 2020.
- LaGrone, Sam, “Milley : China Wants Capability to Take Taiwan by 2027, Sees No Near-term Intent to Invade”, *USNI News*, June 23, 2021.
- Ochmanek, David and Michael O’Hanlon, “Here’s the Strategy to Prevent China from Taking Taiwan”, *The Hill*, December 8, 2021.
- RUSI, *Meatgrinder : Russian Tactics in the Second Year of its Invasion of Ukraine*, May 19, 2023.
- Ries, Eric, *The Lean Startup: How Today's Entrepreneurs use Continuous Innovation to Create Radically Successful Businesses*, Crown Business, 2011
- The White House, *National Security Strategy*, October 2022.
- United States Senate Committee on Armed Services, “Senate Armed Services Committee completes markup of National Defense Authorization Act for Fiscal Year 2016”, press release, May 14, 2015.