Cyber Horizon: AI, Sea Power, and a Potential Taiwan Conflict

Anduril’s Sentry uses artificial intelligence to provide highly accurate, persistent autonomous awareness across land, sea and air. *Credit: Anduril*

In the evolving landscape of 21st-century warfare, the convergence of cyber capabilities, artificial intelligence (AI) and traditional naval operations presents unprecedented challenges and opportunities for the U.S. Navy.

As tensions in the Taiwan Strait escalate, the potential for a cyber conflict between China and the U.S. looms large, with far-reaching implications for global security and economic stability. As Commander Robert “Jake” Bebber argues in his article “Cyber Power is a Key Element of Sea Power” (Proceedings, December 2022), cyber capabilities are now inextricably linked to maritime dominance.

“China has employed cyber-enabled means to shift the balance of global sea power. Its broader neo-mercantilist campaign, spanning more than 60 countries, two-thirds of the world’s population, links land, sea, financial, and digital corridors back to China,” Bebber warned.

This strategy extends to critical maritime infrastructure, with Chinese influence over ports, logistics networks, and global telecommunications posing a significant threat to U.S. naval freedom of navigation and maneuver.

AI has drastically altered naval warfare, placing the U.S. Navy at a critical juncture, according to Paul Scharre in “The Navy at a Crossroads” chapter of the book “AI at War,” published by the Naval Institute Press. Global AI capabilities

have expanded dramatically because of the military robotics revolution, which was fueled by exponential gains in data and processing capacity. Due to their superior vision, pattern recognition, prediction and optimization capabilities, artificial intelligence systems serve as a general-purpose enabling technology. Modern AI systems behave similar to computing or electrical power and are capable of performing a wide range of military missions.

AI helps with predictive maintenance in marine applications, which lowers costs and boosts military preparedness. Additionally, it facilitates data analysis and intelligence gathering, improves logistics and streamlines procedures. With more autonomous support vehicles, these advancements boost military decision-making and combat effectiveness. According to Scharre, AI will mostly be used by unmanned combat systems in naval warfare. The technology is revolutionary for naval operations since it can save energy consumption while increasing operational effectiveness.

Lessons from Ukraine

The ongoing conflict in Ukraine has provided unexpected insights into the role of information warfare and cyber operations in modern conflicts. In a fall 2023 Cyber Defense Review article, authors Chris Bronk, Gabriel Collins and Dan Wallach present several key findings that challenge pre-war assumptions and highlight new dimensions of warfare. With respect to cyber operations and infrastructure resilience, they found that contrary to expectations, Russian cyber activities had less strategic influence than anticipated. This challenges assumptions about the centrality of cyber efforts in kinetic warfare. Ukraine’s digital infrastructure has shown remarkable resilience, attributed to better preparation and support from the global IT industry. Private sector companies like Google and Microsoft have played significant roles in Ukraine’s cyber defense.

Regarding cyber tactics, while large-scale cyberattacks were less impactful, the conflict has seen an evolution. Russian activities have largely been confined to “wiper” attacks that delete critical data and ransomware operations. The integration of cyber capabilities with traditional kinetic operations suggests a more nuanced approach to warfare. In addition, the conflict has underscored the pivotal role of unmanned autonomous vehicles in intelligence, surveillance, and reconnaissance operations. Both cheap commercial drones and more sophisticated unmanned aircraft have proven effective, transforming battlefield situational awareness.

Information warfare has emerged as a crucial aspect of the conflict. Ukraine has effectively dominated the narrative for public support through social media platforms, highlighting its importance in modern conflicts. On the other hand, unexpected communication challenges faced by Russian forces, including failures in encrypted communications, led to the use of unsecured methods, which Ukrainian forces exploited. The growing importance of open-source intelligence has also been demonstrated, with online images and videos providing comprehensive views of the war.

These findings suggest that while cyber operations remain important, their effectiveness can be mitigated by well-prepared defenses and resilient systems. The conflict highlights the increasing importance of information warfare, drone technology, and the integration of cyber capabilities with traditional military operations, with significant implications for future conflicts.

With the defense sector at the forefront of this technology transformation, private sector innovation is becoming more and more important in future naval warfare and cyber operations. Private corporations such as Anduril Industries and Accrete are prime examples of how AI and cutting-edge technology are changing military capabilities, especially in the naval sector.

Anduril’s-Lattice AI platform transforms the way threats are viewed, evaluated and fought by combining data from several sensors to deliver real-time battlespace awareness. Its technologies also include AI-driven battle management systems, counter-drone systems and unmanned systems for improved underwater surveillance – all of which are essential for dealing with new aerial threats. With applications ranging from predictive maintenance to optimal logistics and intelligence gathering, these developments are consistent with Paul Scharre’s conclusions regarding AI’s powers in perception, pattern recognition, prediction, and optimization.

In a similar vein, Accrete is using AI to automate decisions. Accrete’s AI agents are well-known for their ability to reason, learn, forecast and make decisions at scale. They also produce knowledge graphs that condense human tacit knowledge and semantically unite complex data. Based in New York and first established as Mindfire in 2017, Accrete provides services to sectors such as supply chain risk management, social media story analysis and IT service management. Accrete’s AI agents are improving decision-making in the public sector, just like Anduril’s technologies are helping revolutionize naval and cyber operations. With significant ramifications for strategy, security, and operational effectiveness, these developments collectively highlight the vital role that private sector technology plays in developing both military and civilian capabilities.

Attendees observe the Anduril Sentry Tower during the NavalX SoCal Tech Bridge’s Electric and Unmanned Logistics Demonstration on Marine Corps Air Station Miramar, San Diego, California, June 23, 2021. *Credit: U.S. Marine Corps | Lance Cpl. Krysten Houk*

A Future Cyber War

In a future cyber war, there is a hypothetical but potential scenario involving Taiwan.

China might launch a sophisticated cyber-economic assault as an opening move. This strategy would likely aim to disrupt Taiwan’s critical infrastructure, including power grids, banking systems and telecommunications networks. The goal would be to effectively isolate the island and cripple its defenses before any kinetic operations begin.

Drawing from the lessons of the Ukraine conflict, as outlined in “The Ukrainian Information and Cyber War” by Bronk, Collins and Wallach, we can anticipate such an attack would be multifaceted. It might include wiper attacks, ransomware to deny access to essential systems, and targeted disruptions of command-and-control networks. The authors note in Ukraine, contrary to expectations, such attacks had limited strategic impact due to robust defenses and international support. However, China, learning from Russia’s experiences, might employ more sophisticated and overwhelming tactics.

The U.S. response would likely involve a multi-domain approach, leveraging both military assets and partnerships with private sector innovators. The Crowd Strike 2024 Global Threat Report claimed, “We’re seeing the birth of a new kind of warfare, where economic disruption, cyber-attacks and kinetic operations are seamlessly integrated.”

In this scenario, technologies from private sector innovators could prove crucial. Autonomous underwater vehicles could enhance the Navy’s undersea surveillance capabilities, potentially detecting and countering Chinese submarine activities near Taiwan. Counter-drone systems might be vital in defending U.S. ships from swarms of autonomous Chinese drones, a threat highlighted by the extensive use of drones in recent conflicts in Ukraine and the Red Sea. Data-fusion platforms drawing input from multiple sensors could be instrumental in managing the complex, multi-domain nature of such a conflict.

The scenario would likely also involve intense information

warfare, as seen in Ukraine. Both sides would attempt to control narratives, influence global opinion and maintain morale. The U.S. and Taiwan might leverage open-source intelligence and social media platforms to counter Chinese propaganda and disinformation campaigns.

This hypothetical Taiwan scenario underscores the evolving nature of modern warfare, where cyber capabilities, AI-driven systems and traditional kinetic operations are increasingly intertwined. It highlights the critical role of private-sector innovation in national defense and the need for robust, resilient systems capable of withstanding and responding to sophisticated, multi-faceted attacks.

The economic implications of a cyber conflict, particularly in a Taiwan scenario, would be profound and far-reaching. In Bebber's article in U.S. Naval Institute Proceedings from July 2017, "China's Cyber-Economic Warfare Threatens U.S.," he mentions three key sectors at risk – the semiconductor industry, undersea cable networks and maritime shipbuilding, sectors critical not only for economic stability but also for maintaining military technological superiority.

The semiconductor industry is particularly vulnerable. Taiwan produces more than 60% of the world's semiconductors and 90% of advanced chips. A disruption in this supply chain, as noted in "The Ukrainian Information and Cyber War" by Bronk, Collins, and Wallach, could severely impact various industries from smartphones to automobiles and – critically– advanced military systems. For the U.S. Navy, this could mean a significant setback in maintaining its technological edge in areas like AI-driven systems, advanced radar and communications technologies.

Undersea cable networks, through which more than 95% of intercontinental internet traffic travels, represent another critical vulnerability. Cyber-attacks targeting these networks could disrupt global communications, including vital military

command and control systems.

The maritime shipbuilding industry, crucial for naval power projection, is also at risk. Cyber-attacks could delay vessel construction, compromise design integrity or introduce vulnerabilities into ships' systems. This threat is particularly significant given the long lead times and high costs associated with naval shipbuilding programs.

The globalized nature of modern supply chains further exacerbates these vulnerabilities. As seen in the Ukraine conflict, disruptions in one sector can have cascading effects across multiple industries and nations. For naval readiness and national security, this means a cyber-attack on seemingly unrelated sectors could indirectly impact military capabilities. Moreover, the economic warfare aspect of cyber conflicts can include tactics like financial market manipulation, intellectual property theft and strategic acquisition of key technologies and resources. These activities, while not directly targeting military assets, can erode a nation's economic advantages and, by extension, its ability to sustain long-term military operations.

In summary, the economic dimensions of cyber warfare extend far beyond immediate financial losses, potentially reshaping global economic landscapes and fundamentally altering the balance of military power. Understanding and mitigating these risks is crucial for maintaining both economic stability and national security in the age of cyber conflict. As AI and cyber capabilities continue to evolve, the U.S. Navy faces both enormous challenges and unprecedented opportunities.

Success in future conflicts, particularly in a scenario involving Taiwan, will depend not just on ships, aircraft and submarines, but on the ability to dominate the invisible digital domain that underpins modern naval operations. In his Jan. 27, 2021, address to the Naval War College, Admiral Michael Gilday, the former Chief of Naval Operations,

summarized the situation succinctly.

“The navy that masters AI and cyber warfare will control the seas of the 21st century,” he said. “Our mission is to ensure that navy is the United States Navy.”

Moving forward, the U.S. Navy must continue to invest in cutting-edge technologies, foster partnerships with innovative companies and develop adaptive strategies to navigate the interconnected realms of cyber, economic and kinetic warfare.

Joe Greco is the president of the Orange County Council of the Navy League. A professor of global risk management and international finance at California State University, Fullerton, he is a published author contributing to the study of global markets and the U.S. Navy’s command of the seas. In addition to his leadership role in the Navy League, Dr. Greco is an author and member of the U.S. Naval Institute, the American Sea Power Project and the Sons of the American Legion. This article originally appeared in the December issue of Seapower magazine.