Naval Intelligence and Information Warfare in the Gray Zone

An essay submitted to the U.S. Naval Institute for the 2019 Naval Intelligence Essay Contest.

The views expressed herein are those of the author and are not to be construed as official or reflecting the views of the Department of the Navy or the US Government.

July 9, 2019

Words: 2,491

In the Near Future

Amir launched his swarm of drones from his special purpose shipping container that rested atop the neat stack of containers aboard an unflagged commercial vessel. The commercial vessel had been secured through a shell company associated with the smuggling operations of a transnational criminal organization. After a careful transit through the Strait and quiet passage towards the Gulf, Amir's A-hour had finally come. It had been over two years since he left the University of Tehran where he was double majoring in Mechanical and Aeronautical Engineering. Despite his perfect grades and original research in leveraging additive manufacturing for unmanned aerial vehicles customization, Amir left school after becoming radicalized by internet propaganda from the Houthi's struggle in Yemen against the Saudi-led coalition. Today, Amir's swarm of *Qasef* drones targeted the pipeline network carrying oil from the world's most prolific oil field. Each of his 40 medium range drones carried a shaped-charge explosive capable of penetrating the thickest commercial pipe wall. However, Amir's mission was the first of its kind. Unlike the Houthi's in Yemen, Amir had traveled through the Straits of Florida, to the Gulf of Mexico and his target was the Texas petroleum pipeline network. Endorphins flooded his systems as he watched each autonomously piloted drone find its target along the oil, gas and refinery network of Port Arthur, Texas.

Introduction

In a Washington Post op-ed, former US Navy SEAL and Congressman Dan Crenshaw (TX-2) succinctly described US military involvement abroad, "We go there so they don't come here". Congressman Crenshaw's explanation clearly described in one sentence the modus operandi behind the long-standing expeditionary nature of the US national security enterprise. For over two centuries, US strategy has enjoyed the benefits of two ocean sized moats. As long as the military could keep adversaries on the far side of its oceans, life and business in the US could continue in a secure environment. In prior decades an attack on the US required the resources of a nation state or incredibly well funded terrorist attacks such as those of September 2001. Today, non-state actors or proxy groups with minimal funding can launch commercially available drones from civilian ships or pleasure craft and hold the US coast line at risk from outside US territorial waters. The US national security enterprise and its robust intelligence network have accumulated decades of experience countering these gray zone threats far from home, but the proliferation of commercial drone technology has permanently shifted the calculus of national security.

Anticipating the enemy's potential to conduct gray zone activities in the homeland seems daunting, but the Chief of Naval Operations' *Design for Maintaining Maritime Superiority 2.0* provides the needed framework for the Naval Intelligence and Information Warfare (IW) community to prepare the operational environment for such challenges. Maintaining maritime superiority near the homeland will require strengthening naval power, implementing high-velocity methods for intelligence sharing, adequately preparing USN personnel, expanding the traditional network of partners and reinforcing intelligence and IW competencies will be critical enablers in all four lines of effort (LOE). By embracing the Design's LOEs, the intelligence and IW community will be prepared to provide perspective and synchronize the operations of DoD, domestic security agencies and civilian entities in the homeland in order to ensure continued security and economic prosperity for the US.

Strengthening Naval Power

US law places significant limitations on Department of Defense (DoD) assets and activities on US soil. The Posse Comitatus Act of 1878 expressly limits the ability of the military to operate within the homeland in order to prevent the federal government from using the military to force domestic agendas. US legal code further limits the domestic activities of DoD assets in the intelligence collection and analysis domain. Thanks to ocean barriers, friendly neighbors and the previous limitations of enemy technology, the pain points of US law have not significantly prevented defense of the homeland. However, the recent escalations in the southern border crisis highlight the resource and legal limitations of the Department of Homeland Security (DHS) as well as state and local governments. If gray zone actors equipped with commercially available drone technologies chose to exploit the border crisis, the resulting security environment will require the Naval Intelligence and IW community to strengthen its role in defense of the homeland.

The USN's distributed maritime operations (DMO) concept will be critical for strengthening naval power along the US coastline. The concept of operations for the majority of large naval combatants planned to project power far from the US, so the Naval Intelligence and IW community will need to learn to work with new platforms in a joint environment. Since these large combatants will still be needed for power projection far from the home, the lighter cutters of the US Coast Guard (USCG) and expeditionary hardware of the US Marine Corps (USMC) will likely provide a significant portion of resources and personnel for homeland defense scenarios. To ensure interoperability, the USN must continue to invest heavily in its sister services' C4ISR equipment. Common C4ISR equipment will enable improved collaboration among the services intelligence and IW cadres in DMO.

The 2018 National Defense Strategy called for the concept of Dynamic Force Employment (DFE). DFE provides a model that strengthens naval power engaged in DMO. DMO and DFE complement each other because DMO requires leaders who are ready for mission command, which involves leaders to be empowered by their superiors to achieve a given objective with only generic guidance. Such delegation is critical for teams operating in a gray zone environment. Further, intelligence and information professionals must be prepared to operate within command and control (C2) structures where the needed legal authorities reside. For example, certain scenarios might require USN intelligence units to align under USCG C2 since the USCG possesses both national defense and domestic law enforcement legal authorities. By combining the legal authorities of the USCG with the comparatively larger resource base of the USN, the sea services' use of DFE will result in an improved ability to conduct joint operational planning and a more comprehensive and layered defense of the US coast line.

Implement High-Velocity Methods for Intelligence Sharing

Beyond the major muscle movements of aligning personnel, platforms and C2 with appropriate legal authorities, the Naval Intelligence and IW community will need to design and implement a high-velocity operational architecture to support DMO. The priority for this operational architecture will be to provide intelligence support to joint service planners and decision makers as well as federal, state and local law enforcement partners. Additionally, there will be a need to share indication and warning information with US commercial and industrial concerns for situational awareness. While measures will be necessary to protect sources and methods of information gathering, the priority will be to distribute the greatest amount of useful intelligence at the lowest possible classification level. The National Geospatial-Intelligence Agency's "Notice to Mariners" and Federal Aviation Administration's "Notice to Airmen" provide a model of how intelligence and IW professionals can provide maximum support during planning and execution phases.

DMO necessitates that unit leaders operate with a mission command mindset. In order to excel in DMO with high-velocity methods, Naval Intelligence and IW professionals must be practitioners of systems like the Plan, Practice, Perform, Progress and Promulgate (P5) cycle. To aid commanders and units in the execution of the P5 cycle, the sea services must provide the tools, training and authorities necessary to make data driven predictive decisions. The use of such science-based practices will lead to a virtuous cycle in the mission command environment. The data informed P5 cycle will lead to higher quality decisions by unit leaders operating under mission command, which will reinforce trust in leaders performing DMO.

USN personnel will likely be the best trained in P5 methods and provide the most capable marine hardware, but may lack the needed contact layer to provide intelligence support to state and local organizations. Similarly, domestic institutions may lack mechanisms for providing input to Naval Intelligence and IW professionals. The DHS' National Response Framework (NRF) and National Incident Management System (NIMS) provide excellent templates for integrating whole-of-society efforts for natural disasters and isolated terrorist attacks. Naval Intelligence and IW commands should formally codify its plan to support the NRF and NIMS, and the USN should recommend ways to better equip the NRF and NIMS for more complex defensive and offensive action.

Prepare Personnel for the Future

Since the most likely kinetic threat to the US comes from a gray zone attack using commercially available technologies, Naval Intelligence and IW personnel must be ready to integrate into a security environment closer to home. The majority of active duty military personnel are accustomed to operating exclusively within DoD C2 structures, but DoD personnel must be prepared to integrate into non-DoD chains of command to support Defense Support to Civil Authorities (DSCA) and Joint Domestic Operations missions. Additionally, qualified personnel must be prepared to support the intelligence planning process for domestic defensive and offensive cyberspace task forces.

Preparing personnel to support homeland operations can occur at relatively little additional financial cost, but it will require significant time to hone relevant skill sets. To facilitate the needed credentialing, active and reserve intelligence and IW professionals must leverage block learning to receive ready and relevant training. DHS provides a significant library of pre-built NRF and NIMS training products for no cost, and the National Guard Bureau (NGB) and US Northern Command have numerous high-quality training products concerning DSCA. Conveniently, state and local governments as well as commercial concerns already participate in the NRF and NIMS training program. By using these standardized products, USN personnel will gain fluency in the language of domestic agencies and participating commercial concerns. As a result, intelligence and IW units will be able to translate the joint intelligence process to domestic partners. Lastly, while the overwhelming majority of USN personnel belong to the active component, the DSCA and Joint Domestic Operations mission sets provide an excellent opportunity to align the Navy Reserves to operational tasking, instead of administrative roles.

To fully prepare for the future, the USN must update its Navy Family Framework for probable threat scenarios. In recent decades, family preparedness inside the continental US has been mostly limited to natural disaster avoidance and basic operational security measures on social media. Since homeland attacks will require mobilization of service members who may have family members at risk, the Navy Family Framework must be resilient. Examples of resilient family readiness models exist at forward deployed DoD bases, USCG Search and Rescue stations and domestic law enforcement agencies.

Expand the Traditional Network of Partners

Beyond its sister sea services (USCG and USMC), the Naval Intelligence and IW community must reinforce relationships with military counterparts in the US Army (USA), NGB and US Air Force (USAF) and respective reserve components. In addition to improving collaboration with joint partners, the USN should identify useful spare capacity within the DoD's infrastructure to ensure agile, geographically mobile and resilient intelligence support. At the service level, the USN should consult with the Base Realignment and Closure Commission and refer to the Base Redevelopment and Realignment Manual on available spare capacity and methods for repurposing in the event of domestic mobilization.

The Naval Intelligence and IW community is deeply integrated with the 17 members of the Intelligence Community (IC). However, within the gray zone numerous other federal agencies may possess the most valuable expertise and legal authorities, so inter-organizational collaboration will be decisive. For example, the IC may rely on information from the Federal Aviation Administration to assess the threat posed by commercially available drones. Additionally, coordination over radio spectrum allocation with the Federal Communications Commission and the National Telecommunications and Information Administration may be critical in disabling the communication methods of remote or autonomously piloted drones without jeopardizing commercial air traffic or cellular communications.

The USN must deepen integration with state, local and tribal authorities. In addition to standardized training provided such as that provided by NRF and NIMS, the USN must develop cooperation agreements with various levels of government and industry. The Naval Postgraduate School's Center for Homeland Defense and Security provides an excellent example of how the intelligence and IW community can engage in advance with local communities and industry to map potential demands, threat response and information sharing capabilities. Additionally, flexible Memorandums of Agreement (MOA) must be pre-negotiated negotiated in order to best serve the homeland after crisis initiation. In addition to MOAs, the USN must identify or create financial vehicles similar to Other Transaction Authorities that can rapidly equip active duty members or mobilized reservists for unplanned scenarios.

Beyond national borders, the intelligence and IW commands must codify principles of multinational intelligence sharing with foreign national counterparts of friendly countries within the western hemisphere. Security cooperation and information sharing with Canada and Mexico will be the most critical. Beyond immediate neighbors, the USN must coordinate with partner nations to fully map threats and develop planned responses. The USN should identify ways to strengthen existing multinational exercises such as PANAMAX (defense of Panama Canal) and identify new exercises that will prepare combined intelligence support teams for gray zone conflicts. To support increased information sharing with the broadest number of partners, the USN should consider using US Central Command's "Middle East Stabilization Force" (MESF) tetragraph as a model for sharing information with an increased number of partners. Finally, multinational intelligence and IW teams must provide threat assessments and vulnerability analysis for a range of operations in cyberspace in order to protect critical infrastructure such as transnational oil and gas pipelines from drone attack.

Conclusion

In *Team of Teams*, General Stanley McChrystal (USA, retired) recounted the reinvention of the Joint Special Operations Task Force into an agile organization that could evolve as fast as the insurgent enemy in 2004 Iraq, “We had to tear down familiar organizational structures and rebuild them along completely different lines, swapping our sturdy architecture for organic fluidity, because it was the only way to confront a rising tide of complex threats”. McChrystal’s principles directly apply to the Naval Intelligence and IW community as the US prepares for gray zone threats at home.

The Naval Intelligence and IW community must learn and adapt faster than our rivals in order to assure maritime superiority in the approaches to the homeland. The USN, sister military services and domestic agencies are well staffed, equipped and funded to prevail against the emerging threats, but all parties must identify existing pathways to collaborate in the fastest and most efficient ways possible. Critically, this will require formal communication pathways with civilian and commercial concerns in order to ensure continued security and economic prosperity. Maintaining maritime superiority near the homeland will be a critical element for defending against the coming gray zone threats. By strengthening naval power, implementing high-velocity methods for intelligence sharing, adequately preparing personnel and expanding the traditional network of partners, Naval Intelligence and IW teams will be prepared to ensure continued security and economic prosperity for the homeland.