Cyber Reconnaissance

Focusing on the adversary

by Maj Allison Warwick & CWO2 Christopher DiPalma

>CWO2 DiPalma is a 2602 Signals Intelligence/Electronic Warfare Officer/Cyber Operations Officer currently serving as the Future Operations Officer, Battalion Training Officer, and Computer Network Exploitation Officer-in-Charge at 2d Radio Battalion.

>>Maj Warwick is a 0202 Marine Air Ground Task Force Intelligence Officer currently serving as the Information Warfare Company Commander at 2d Radio Battalion.

The Marine Corps must prioritize and maximize our understanding of adversary actions within the challenging domain of cyberspace in order to counter, exploit, and dominate near-peer threats. *MCDP 1, Warfighting,* tactics and principles apply to actors resident in the logical and persona dimensions of cyberspace as much as within the exclusively physical warfare domains. The "changing face of war" requires us to modernize, adapt, and innovate to win.[1] William S. Lind reminds us that maneuver warfare is not a new concept; modern day warfare requires us to think spatially, creatively, and critically to avoid fixed, predictable, and telegraphable schemes.[2] Applying American psychologists Joseph Luft's and Harry Ingham's Johari Window Model to the cyber warfare domain by manipulating and intentionally positioning our tactical, organic infrastructure and capabilities (reconnaissance assets) to not only defend but to observe could strategically enable us to gain insight into our blind spots.[3] Observation of enemy activity can allow for rapid response to crisis and rapid transition from the defensive to offensive operations in the form of a counter attack. Cyber-reconnaissance techniques, such as Digital Network Intelligence analysis contained in the traditional concept of Intelligence Preparation of the Battlespace and Cyber Intelligence, Surveillance, and Reconnaissance, provide a systematic methodology to define the cyber landscape by mapping and observing adversary actions to support operational planning efforts. Understanding the dimensions of the cyberspace warfare domain and applying traditional warfare concepts to it is crucial to the modern-day warfighter's success in competition and in conflict with near-peer adversaries.

The Need for Cyber Reconnaissance

We need not look far to forecast the potential future effects that our adversaries' cyber-reconnaissance efforts could wage against us across all warfare domains, further necessitating our aggressive actions within the same domain. In 2017, alleged Russian cyber hackers released NotPetya onto Ukrainian Linkos Group's update servers, with devastating impacts totaling an estimated $10 billion across multiple corporations. This attack crippled Maersk shipping and FedEx's European subsidiary in particular.[4] How exactly did the alleged Russian hackers engineer this attack? Through reconnaissance activities, knowledge of routine server updates on Linkos' servers provided an opportunity and a vehicle for rapid malware delivery to their intended targets. More recently, in May of 2021, DarkSide held Colonial Pipeline hostage at a bitcoin ransom valuing over $5 million while threatening a data breach of sensitive information should the company not pay the ransom. This hack against America's largest fuel pipeline paralyzed east coast U.S. energy distribution, resulting in public panic over gas shortages.[5] This particular example concluded when Colonial Pipeline reportedly paid the ransom in full.[6] These examples only underscore vulnerabilities in cybersecurity defenses, the ambiguity of how the U.S. Government and the DOD define cyber-criminal acts, and challenges associated effective responses to cyber criminals within the cyber domain. Now, think about the cost of our tactical inaction in the cyber domain when it comes to protecting our nation's military branches, corresponding weapon systems, capabilities development, and network infrastructure.

There Are Existing Models to Understand and Get After the Adversary in the Cyberspace Domain; We Just Need to Recognize and Apply Them

A critical step in enabling the Marine Corps to influence the adversary, in accordance with the friendly forces' endstate, is pursuing relentless, aggressive reconnaissance across all warfare domains. Reconnaissance helps us to identify vulnerabilities, gaps, and exploitable opportunities. When it comes to reconnaissance, perhaps a universally understood Marine Corps analogy to draw is from within the infantry in support of ground combat operations. The best way to find out what is in that valley is to go over there and see what is in

it. Similarly, if we want to know what is on the other side of that obstacle (in this case a firewall), there is a way to find out.

In the traditional warfare domains, we would never allow our forces to hunker down in defensive positions without pursuing and manipulating the enemy to break his will to fight. During World War I, the Allied Powers, in static defensive positions along the Western Front, made little and often insignificant or short-lived forward progress against the enemy until they were able to overcome the lethality of the combined arms effects brought about by machine gun and artillery fires. Forces only truly overcame these technological military advances by means of resource attrition, a tactic absent in modern day warfare. Once sufficient attrition had been achieved, only then did the advent of new maneuver warfare tactics and the utility of tanks supersede the previously impenetrable wall of static defensive positions supported by combined arms effects.[7] Any course of action that would rely on the attrition of our current adversaries' resources to impact their capabilities in cyberspace would be not only costly but would represent an overestimation of our current capability to affect our competitors. However, the key difference when relating current cyber threats to the drastic technological advances of the early 1900s is the concept that the Allied Powers' warfighting capabilities were on par with that of the Triple Alliance along the Western Front, which facilitated the nearly four years of defensive stalemate. In the current cyber domain, we may be critically behind our competitors with regard to our ability to effectively use cyberspace technological advances to conduct defensive or offensive cyber operations in such a way as to force a stalemate.

To break this stalemate, we must not only identify the adversary centers of gravity and critical vulnerabilities (within the cyber domain or by means of cyberspace operations) but use these same reconnaissance techniques to better understand our own vulnerabilities from the cyberspace perspective. According to GEN Paul Nakasone, Director U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Services, those who seize the initiative in cyberspace also seize the advantage. GEN Nakasone refers to the activity conducted external to friendly networks as "defending forward," or enabling future outcomes to shape the enemy in line with the friendly scheme of maneuver. Persistent presence is required to operate effectively in the future cyberspace fight. Friendly forces must aggressively pursue action to understand enemy actions and track our adversaries in cyberspace.[8] In other words, and similarly to any other prepared defensive position, the most effective method of employment would be a defense-in-depth strategy coupled with aggressive cyberspace "patrols" outside of the cyberspace defensive "perimeter." These aggressive actions would allow friendly forces to remain cognizant of adversarial posturing activities in order to enhance the ability to defend and attack. Most importantly, this course of action provides the option to choose when to defend or when to attack rather than respond to threats retroactively.

Persistent presence is required to operate effectively in the future cyberspace fight.

Dually beneficial to both protecting friendly networks and gaining knowledge of adversary composition, disposition, and strength, cyber-reconnaissance enables the tactical warfighter to preempt weak defenses and capitalize on exploitable opportunities. In the cyber domain, MITRE defines reconnaissance as the first step in enabling the cyber-attack lifecycle, which includes both opportunities for exfiltration of valuable information (intelligence gain) and disruption operations (Offensive Cyber Operations):

> Attacks in cyberspace are no longer limited to simple (albeit significantly harmful) discrete events such as the spread of a virus or worm, or a denial-of-service attack against an organization. Campaigns are waged by the advanced persistent threat (APT), following a cyber-attack lifecycle. Campaigns involve stealthy, persistent, and sophisticated activities, to establish a foothold in organizational systems, maintain that foothold and extend the set of resources the adversary controls, and exfiltrate sensitive information or disrupt operations.[9]

We can apply this lifecycle concept to cyber-reconnaissance methods with relative ease. Unmasking the enemy's concealment behind aliases, social engineering methods, and operational security measures exposes key terrain within cyberspace for us to leverage. "Local security patrols" in the cyber domain can be sent to areas as a feint for kinetic actions launched in a different direction. To use another common ground defensive tactic, listening posts/observation posts help us sense and detect enemy activity in order to alert our forces to potential danger to provide a defense in depth for a prepared position. Military staffs, in particular intelligence sections, apply the process of intelligence preparation of the battlespace to the cyberspace domain in a highly technical manner to map the cyber landscape and identify opportunities to support operational planning.

II MEF Information Group's Pursuit of the Adversary

One application we have learned at II MIG is the seamless integration between Defensive Cyberspace Operations (DCO) and intelligence units. A clear focus on processes allows teams to collaborate to complement each other's end states, while building domain-specific expertise in respective functional areas. The application of traditional maneuver warfare concepts to the cyberspace warfare domain is endless. Taking this concept one step further, multiple information capabilities can participate in cross-domain competitive acts to further enhance actions on target. For example, Defensive Cyberspace Operations identifies known actors who attempt to penetrate friendly networks and can enable attribution in the form of public mes-

saging to "name and shame" the adversary, thus capitalizing across domains.[10] In a recent exercise, DCO-Internal Defensive Measures Company established named areas of interest around critical terrain, typically a network boundary shared by two organizations. They conducted reconnaissance missions to confirm or deny adversary presence. In one instance, DCO-Internal Defensive Measures Company discovered adversary attempts to cross that boundary and applied fused intelligence capabilities to determine the specific actor, not only to increase our understanding of the actor(s) operating against our tactical networks but also offer options to other cyber mission forces to understand that threat. This situation allowed for II MIG to interface with national and theater level assets, which enhanced national tactical integration and began to define a clearer process to navigate the DCO to Offensive Cyber Operations handoff. But what if tactical units not only attributed known actors but *uncovered* and attributed previously unknown actors, keeping the knowledge of our "blind spots" close hold in order to fuel our deliberate targeting cycle? What if we crafted an intentional, controlled chink in our armor, intended to enable the enemy's reaction and observe tactics, techniques, and procedures to further harden and safeguard friendly networks?

In addition to intelligence and targeting gain, an element of cyber reconnaissance can also be applied to military deception operations. Once we turn the tables on the problem set and understand how the enemy perceives our vulnerabilities and strengths, we can manipulate the enemy's avenues of approach to our advantage. Once again, operations in the cyberspace domain look different yet necessitate the same principles of maneuver warfare to defeat the enemy. Counter-surveillance operations in the cyber domain require detailed analysis, assessment, and dedicated focus to identify opportunities. Misleading the enemy about our friendly-force structure may lead to improved detection methodologies, proactive defensive measures, and deliberate targeting efforts.

Though physical warfare domains enjoy a relative amount of detectable and predictable action in times of peace, operations in cyberspace are in constant motion and persistent competition at all times—necessitating our focus in the area. Critical information requirements of operations in the information environment do not differ from critical information requirements when compared to land, sea, or airbased combat operations. It is essential to comprehend that capabilities and limitations of our adversaries' kinetic weapon systems and the non-kinetic, cyberbased weapons are no different. These elements should be treated with the same amount of priority and concern due to the potential high stakes impacts to friendly communications, friendly intelligence collection methods, operational security, navigation, weapons systems command and control, and our heavy reliance on automated capabilities that would cripple us if the enemy denied or exploited them. We should actively seek to identify these unknowns about our adversaries to enable us to go toe-to-toe in competition with them across all warfare domains.

Collective Service Actions to Increase Operational Capability in Cyberspace

As warfighters, we should remember that risk is equally present in both action and inaction.[11] The enemy operates largely unchecked in the cyber domain, whereas our current friendly forces balance risk aversion with capitalizing on traditional intelligence gain while maintaining our own non-attribution. This situation creates a challenge to answer tactical requirements and priorities. Cyber capabilities are rapidly available and constantly evolving, which further enable actors to take bigger risks in logical dimensions than in physical dimensions. Enemies face minimal repercussions for their offensive cyber actions because of challenges associated with attributing and prosecuting actors appropriately and in a timely manner. As GEN Nakasone explains, we gain the advantage in cyberspace by taking and maintaining continual action.[12]

The question on everyone's mind is: *how* does the Marine Corps position ourselves for success within such a tumultuous domain? The very top priority if we want to graduate to "varsity-level" operations in the cyber domain needs to be technical training and proficiency across the intelligence disciplines, cyber MOss, and MIG functions. Digital Network Intelligence in support of Cyber Intelligence Preparation of the Battlespace requires technical training, experience, and a thirst for knowledge as tools and capabilities modernize rapidly. At II MEF, we are already focusing our efforts towards developing, sustaining, and growing our technical capacity. In addition, and recognizing technical proficiency as a top priority, Marine Forces Cyber Command is already taking steps to stabilize Marines on station for longer duration tours to offset the technical and tactical proficiency required to work alongside national level agencies in order to achieve mission success for the Marine Corps.

Second, national- and tactical-level organizations need to realign and reprioritize efforts to enable America's military branches to take requisite actions in the cyber domain. The current posture of Marine Corps cyber assets and personnel with the training and authorities to conduct this level of reconnaissance in cyberspace does not support the operational priorities of any MEF, nor are they tasked in such a way to shift focus as needed. A "cyber call for fire" would require each MEF to coordinate with a sister Service cyber component, whose tasking is based on NSA mission alignment—and for a completely different strategy—to provide information and intelligence to national policy and decision-making entities. Even in the best-case scenario of an established working relationship with these sister Service cyber components, current authorities would not allow for these activities to support MEF priorities. Any support provided would be in the form of research and reporting marginally related to MEF requirements and would not allow for direct, continued reconnaissance activities on behalf of MEF operational planning. To put it simply, there are currently no task organized cyberspace reconnaissance assets available to the MEFs for tasking to gather intelligence on the enemy for opera-

tional planning purposes. The current alignment will not enable the Marine Corps to answer tactical requirements to protect and defend our tactical networks while exploiting opportunities on the offensive.

Conclusion

As in any domain, combined, joint, and national efforts are how we win. Enhancing synchronization between MEF-level defensive operations and strategic Offensive Cyber Operations will allow for the rapid response and deployment of desired effects against known adversaries. Understanding adversary actions within the cyberspace domain will enhance our knowledge of adversary intent and priorities across all domains. Ultimately, those who are reticent to arrange for and make reconnaissance in the cyberspace domain should consider the positive impacts of precise, combined actions contained within cyber-reconnaissance methods to support the tactical warfighter

Notes

1. Headquarters Marine Corps, *MCDP 1, Warfighting,* (Washington, DC: 1997).

2. William Lind, *Maneuver Warfare Handbook*, (New York, NY: Taylor & Francis, 1985).

3. L. Garagna, "Seeing through the Johari Window: Improving the Quality of Interpersonal Communication," (Paper presented at PMI® Global Congress 2003-EMEA, The Hague, 2003).

4. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, (August 2018), available at https://www.wired.com.

5. Jessica Resnick-ault, "Colonial Pipeline Ramps Up as U.S. Seeks to Emerge from Fuel Crunch," *Reuters,* (May 2021), available at https://www.reuters.com.

6. William Turton, Michael Riley, and Jennifer Jacobs, "Colonial Pipeline Paid Nearly $5 Million Ransom to Hackers," *Bloomberg,* (May 2013), available at https://www.bloomberg.com.

7. Martin Van Crevald, *The Changing Face of War: Combat from the Marne to Iraq*, (Novato, CA: Presidio Press: 2008).

8. Staff, "An Interview with Paul M. Nakasone," *Forum JFQ 92*, (Washington, DC: National Defense University Press, 2019).

9. Eric Hutchins, Michael Cloppert, and Rohan Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," (Bethesda, MD: Lockheed Martin, 2013).

10. Headquarters Marine Corps, *MCDP 4, Competition*, (Washington, DC: 2020).

11. *Maneuver Warfare Handbook.*

12. "An Interview with Paul M. Nakasone."