Leveraging Cyberspace

Reconnaissance and counter-reconnaissance in the information environment

by Capt Michael Holdridge

The Watch Officer for the MEB Operations Center attempts to log in to his NIPR computer but receives an error stating his account is locked because of excessive failed login attempts. He angrily calls over to the Communication Help Desk, stating that he had just come on shift and had not attempted to log in yet. The Help Desk Marines re-enable his account, and he successfully logs on. When he checks his inbox, he finds a few unread emails that he did not recognize from the day prior. At the same moment, he hears the G-4 Operations section calling down to the CLR to ask why the infantry regiment never received its ammo and fuel resupply. He overhears the MEB Surgeon talking about CASEVAC flights being cancelled without reason. When he looks at the common operating picture, he realizes that the delayed resupply caused the eastern flank for the infantry regiment to become exposed. Simultaneously, he overhears a report of troops in contact from within the rear area.

Unbeknownst to the MEB watch officer, the adversary had gained access to the MEB communications network and had stolen his log in credentials. Using his credentials, the adversary leveraged the unclassified logistics programs to cancel the resupply for the infantry regiment. Additionally, the adversary sent false weather reports sent to the Marine Air Wing, grounding CASEVAC flights that caused a lengthy delay to life support for the troops in contact. The adversary also leveraged access to these logistics programs to identify staging areas for combat service support and gaps in the front line. With this knowledge, the adversary sent special operations forces to penetrate friendly lines and attack the ground lines of communication in these now-exposed areas.

>Maj Holdridge is the 2d MARDIV G-6 Operations Officer. He was previously the Commanding Officer for Company C, 8th Communication Battalion.

This vignette demonstrates the possible results of the invisible reconnaissance that occurs on the front lines of the information domain on a daily basis. It reveals the very real way that operations in the information environment can impact the kinetic battle and operations across the land, air, space, and sea domains. In the scenario, the failure to investigate the account access issues and suspect emails caused the MEB to overlook a gap that the adversary was actively exploiting. The end result of this critical gap leads directly to mission failure. Within the Marine Corps, the MEF Information Group is leading the charge to address these gaps head on by strengthening the relationship between the 17XX Cyberspace Operations, 02XX Intelligence, and 06XX Communication occupational fields. For the Marine Corps to succeed in the era of great power competition, the Service must continue to increase the synergy between communicators and defensive cyberspace operators to better enable both reconnaissance and counter-reconnaissance.

Two recent incidents demonstrate the importance of the synergy between communication elements and cyberspace: the NotPetya attack in Ukraine in 2017 and the 2021 Colonial Pipeline Ransomware attack.[1] The NotPetya attack was a cyberattack targeting civilian and government users in Ukraine that leveraged the Eternal Blue exploit: a National Security Agency tool that the hacking group Shadow Brokers stole in 2017.[2] The Eternal Blue exploit is a vulnerability in Microsoft's Server Message Block Protocol that tricks a breached system into allowing illegitimate traffic into the network. Once the Eternal Blue tool was stolen, the National Security Agency alerted Microsoft, who then released a patch in March 2017 that addressed the vulnerabilities.[3] The impact of NotPetya in Ukraine was immediate, as the attack wiped data from banks, energy firms, government officials, and an airport.[4] The attack crippled and froze domestic functions

For the Marine Corps to succeed in the era of great power competition, the Service must continue to increase the synergy between communicators and defensive cyberspace operators ...

at all affected entities within Ukraine and caused major difficulties for the Ukrainian government in managing the ongoing conflict with pro-Russian Separatists in the Donbass region.[5] This attack demonstrated that the cyberspace domain is not limited to geographic borders, a theater of operations, or an area of responsibility. Our adversaries do not have the same reluctance to target civilian infrastructure, non-military targets, or even their own citizens. All targets are fair game.

The 2021 Colonial Pipeline hack, which impacted oil distribution across the Southeastern United States, was the result of a compromised password leaked onto a hacker forum.[6] Compromised passwords are often leaked across the dark web, a series of difficult to find web sites designed to promulgate hacking tools and is a common source of intelligence for cybersecurity firms. Additionally, during the course of the Colonial Pipeline investigation, it was found that Colonial Pipeline did not use multi-factor authentication, an account access method that requires more than just username and password, such as a text message to a phone in the case of many banks or the use of a log on token for government computers.[7] Multifactor authentication is a basic cybersecurity tool that has been used for decades and is a common security practice by network administrators worldwide.

Neither of these incidents involved direct kinetic attacks between the perpetrators and the victims, but both possess the same devastating ability to shape the battlefield below the level of armed conflict. These attacks serve as a warning to what we will shortly face on the modern battlefield: cyberattacks designed to damage our ability to communicate and conduct basic operational and support functions, to gain intelligence on our operations, to shift our focus, and to disorient our military. As the Commandant has already pointed out, "the answer to the question of how we may best support the broader effort, it seems increasingly likely, is not lethal fires as an end themselves but rather *reconnaissance and counter-reconnaissance* applied in all domains and across the competition continuum."[8]

Most importantly, however, these attacks could have been completely mitigated through a concerted approach to preventing cyberattacks. Both intrusions relied upon vulnerable systems that already had fixes in place. Without the network and system administrators to apply the patches, and without a defensive cyberspace capability to assess the threat environment and the intelligence teams to gather the relevant information, the victims of NotPetya and Colonial Pipeline were left unaware of the risks they faced. If Colonial Pipeline and Ukraine had those teams in place, like the DOD currently does, they could have prevented these attacks from occurring in the first place.

Before We Go Any Further, Some Definitions

To fully understand the impact of these cyberattacks, it is important to understand what ransomware attacks are. Ransomware, as seen in the Colonial Pipeline incident, is an attack where in which an adversary infiltrates a system, encrypts all of the data, and then ransoms the data to the owners. The encrypted data can be anything from an individual user's emails to the operating system files required to run the device. By encrypting this data, an attacker can then deny a user access to the system or device until a fee is paid. All ransomware attacks start with an adversary gaining access to a system. Common methods of gaining access include through social engineering, which is the process of gaining access through tricking someone into providing log in information, or by using an exploit, such as a Zero Day. A Zero Day exploit is a previously unidentified vulnerability for which the manufacturer of the program or operating system does not have a patch or fix. Once a Zero Day is identified, manufacturers will quickly design a patch to prevent perpetrators from using them in the future. Once inside the system, attackers can gather intelligence, steal information, manipulate information, or otherwise operate undetected until they are found and their access removed.

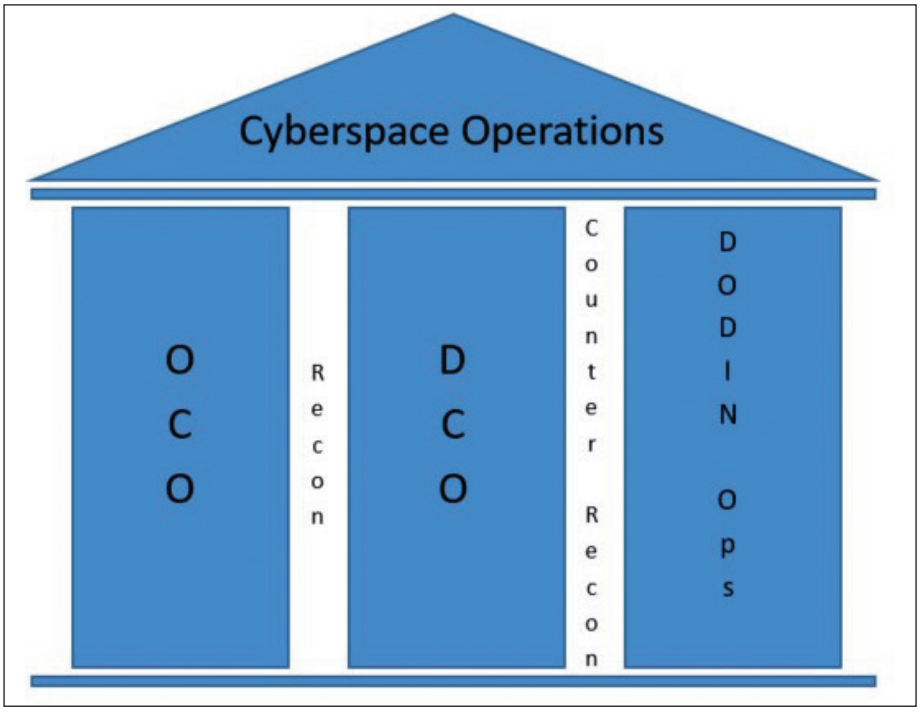
The cybersecurity and defensive cyberspace operators have different roles when it comes to patching in response to a previously identified vulnerability or in responding to a true Zero Day. In the event of a previously identified vulnerability, the network and systems administrators who fill the duties of the cybersecurity professional are responsible for applying the patches and searching for indicators of compromise on the network. The cyberspace defense operators are responsible for assessing the intelligence from the threat environment, providing recommendations to the administrators, and assessing the overall protection level of the network. In the event of a true Zero Day, the defensive cyberspace operators are responsible for hunting, isolating, and gathering intelligence on the intrusion while providing recommendations to the network and systems administrators to fix the network security. Without both of these elements operating in sync, networks will remain vulnerable and the response timeline for the eventual intrusion will increase, which results in more damage occurring.

What Is the Difference Between Cybersecurity and Cyber Defense, and What Is Synergy Between Them?

The DOD is currently postured in a three-column approach to deterring cyberattacks: Offensive Cyberspace Operations, Defensive Cyberspace Operations (DCO), and Department of Defense Information Networks (DODIN) Operations (DODIN Ops). The 0600 occupation field is focused on the DODIN Ops portion of cyberspace operations, specifically on the on the planning, installation, security, operation, and maintenance of communication architectures. The 1700 occupation field has the responsibility for Offensive Cyberspace Operations and DCO, with the 1721, Defensive Cyberspace Operator, supported by the 1702, Cyberspace Operations Officer, having a primary focus on DCO. The difference between DCO and DODIN Ops can be summarized with the following statement: DODIN Ops is responsible for a threat agnostic but threat informed security posture, while DCO is an intelligence driven investigative, as well as command and control function, body working

against an identified specific anomaly or threat. In practice, this equates to the following: DODIN Ops secures the network and any suspicious activity is routed to DCO to investigate and, if identified as an actual threat, neutralize that threat.

The risk that arises with this three-column approach is the space that exists between them. While DODIN Ops and DCO are separate functions, they need to be closely aligned in order to ensure that the security and defense of the network is synchronized. Without the DODIN Ops support to apply changes to the security posture of the network, DCO is unable to truly eliminate a threat once it is identified. Without the intelligence and recommendations provided by DCO, DODIN Ops is unable to secure the network against the specific threats it faces.



Reconnaissance and counter-reconnaissance in the context of the pillars of cyberspace operations. *(Graphic provided by author.)*

What Is the Way Ahead?

As the DOD ramps up its cyber defense in response to increasing threats and invests heavily in the evolution of defensive cyberspace operations, it is worth noting that the first line of defense against these attacks is not the 1700 community but the 0600 community. The 0631 Network Systems Administrators and 0671 Data Systems Administrators throughout the Marine Corps are the primary MOSs responsible for the security of our systems and for patching previously identified vulnerabilities. However, the biggest risk that we face in current practice is the fact that our threat agnostic defense is often a *threat uninformed defense*. In other words, while a vulnerability may be listed as medium risk by the Defense Information Systems Agency (DISA), it may also be a tactic, technique, or procedure (TTP) that is frequently employed by an adversary involved in our area of operations. In that situation, a threat formed approach would grant a higher priority for patching than a vulnerability listed as critical by DISA that is not a TTP of that specific adversary. Traditional DODIN Ops uses a checklist to address the most dangerous vulnerabilities rather than the most likely vulnerabilities. The solution to this is to improve the synergy of the defensive cyberspace analysists and the cybersecurity administrators by facilitating the relationship between these units in order to increase information sharing, intelligence gathering, and threat response. The defensive cyberspace analysists have access to the intelligence resources to identify which advanced persistent threat, or specific adversaries that contain "sophisticated levels of expertise and significant resources,"[9] may be active in a region as well as the TTPs associated with those advanced persistent threat. Furthermore, increased synergy between the DODIN Ops and DCO teams enables the network administrators to assist DCO is intelligence gathering and reverse targeting of adversary teams through the use of various tools and network changes.

Currently, the synergy between DODIN Ops and DCO is not where it needs to be. Rarely do the DODIN Ops Marines responsible for maintaining the cybersecurity posture receive relevant intelligence briefs in order to prepare them for operations. This causes significant delays in response and can lead to disastrous consequences like NotPetya and Colonial Pipleine. The correct actions for a synergistic operation would include the following: along with the usual intelligence preparation of the battlespace, the defensive cyberspace intelligence analysts would provide an additional intelligence preparation of the information environment, to include the cyberspace threat actors active in the region. The cyberspace intelligence analysists would review which peer adversaries were likely to be active, which friendly systems are at risk, and which exploits are likely to be used against U.S. forces. The intelligence analysts would also prepare a threat briefing to the G-2, G-3, and G-6 about the risks in the area and which advanced persistent threats belonging to which country would be in play.

Using this information, the defensive cyberspace intelligence analysts and the DODIN Ops community would prepare a threat informed security environment, with a focus on patching vulnerabilities likely to be exploited. This is much more threat focused and relevant than the typical critical, high, medium, low risk assessment included within the information assurance vulnerability alerts provided by the DISA. Once the security posture is in place

to counter an identified adversary, the Systems Control Center (SYSCON), which monitors, maintains, and changes the communication architecture and is staffed by the 0600 personnel, and the Cyberspace Defensive Operations Center (CDOC), which commands and controls the investigation of network anomalies and mitigation actions and is staffed by the 1700 personnel, would have a synergistic relationship. This would enable the staff to address every anomaly and vulnerability as a team to fully analyze the potential threat and response action.

Some leaders argue that the 1700 community does not require the 0600 community to conduct cyberspace operations. Other than the network being established, what benefit does the 1700 community gain from the 0600 community? It is a fair question, especially since the 0600 community will always create the network to enable commanders to execute C2 across the battlespace. Much of the intelligence gathered by the 1700 community is often at the top-secret level, which is above the security clearance required by the vast majority of the 0600 community. Additionally, since DODIN Ops focuses on a threat agnostic security posture, the specified threats posed by adversaries are rarely addressed by the 0600 community. However, as discussed earlier, this results in a *threat uninformed* and therefore vulnerable network architecture. Furthermore, the 1700 community lacks the ability to implement network and systems changes in the architecture in order to mitigate specific exploits discovered.

There are two main benefits of the 0600 community to defensive cyberspace operations: the implementation of changes on the network to respond to a threat, and the understanding of the network as a whole. The majority of the network changes that are required by defensive cyberspace operations against a specific threat are implemented by the network and systems administrators that the 0600 community owns and develops. Without the administrators to patch systems, update the architecture, and create mitigations, the 1700 community is unable to successfully defend the network against identified threats. But most importantly, the communication officer and communication chiefs have the specific requirement built into their billet and training to translate commander's operational priorities into communication plans that enable command and control. This means that communication officers and chiefs, by necessity, must be able to effectively understand and translate the risks identified by cyberspace focused intelligence. Without that synergy between the communication officers, communication chiefs, and the defensive cyberspace intelligence analysts, it is difficult to translate threats to risks, understand when risk is unavoidable, and identify

additional mitigation that improve the chance of operational success.

Conclusion

The relationship between DODIN Ops and DCO already exists within II MEF. The CDOC, as a component of the Information Command Center and the MEF SYSCON, both manned an operated by 8th Communication Battalion Marines, already have a relationship due to the proximity of command. The MEF Network Operations Center already has defensive cyberspace operations liaisons located within their structure. The intelligence section within the MEF Information Group Information Command Center already synthesizes the intelligence requirements identified within an area of operations. However, as demonstrated by the significance of cyberattacks throughout the world, movement needs to be made to ensure that these two occupational fields are more closely aligned than ever, with a focus on closing the space between DCO and DODIN Ops. Without a clear threat picture provided by cyberspace intelligence analysists, patched systems provided by the network and systems administrators, and the investigative and response actions by defensive cyberspace operators, the Marine Corps places itself in a position of significant risk. But most importantly, in the question of providing cybersecurity to the MEF and in conducting reconnaissance, counter-reconnaissance and counter-exploitation of our networks, the synergy between the 0600 and the 1700 community must be nourished, grown, and strengthened. When the synergy between the 0600 and 1700 community is maximized, the opening vignette would have proceeded very differently:

The Watch Officer for the MEB Operations Center attempts to log in to his NIPR Computer but receives an error stating his account is locked because of excessive failed log in attempts. He angrily calls over to the Communication Help Desk, stating that he had just come on shift and had not attempted to log in yet. The Help Desk Marines register the anomalous activity of a locked account without login attempts to the SYSCON. The SYSCON Watch Officer logs the issue with the CDOC, which begins investigation into the anomaly. The DCO Marine investigates the issue and discovers a breach in the network which is impacting the logistics supply chain resulting in manipulated logistics requests and weather reports. The DCO Marine identifies that an adversary had compromised login credentials for the MEB Operations staff allowed the adversary to manipulate data and harvest intelligence within the MEB NIPR network.

After analyzing the specific threat vector used, he begins to hunt for the perpetrating unit. After receiving approval from the MEB G-6 and Information Control Center, the CDOC and SYSCON work together to establish a cyber-operations approved honey-pot; a collection point designed to lure in the adversary to gather intelligence. Once the adversary is identified, the CDOC provides recommendations to the SYSCON, which coordinates with the MEB G-6 to implement network changes to protect the network. The Network Systems Administrators update the MEB firewalls to limit adversary traffic into the network and the Data Systems Administrator update the Assured Compliance Assessment Solutions scanners to search for specific indicators of compromise. The CDOC provides information to the Cyberspace Intelligence Analysts who are able to connect the TTPs for the specific threat vector used, along with information from the honey-pot, to identify specific adversary units involved. This information is then provided to the Information Operations Center which provides recommended targeting solutions to the MEB G-3 for action.

… in conducting reconnaissance, counter-reconnaissance and counter-exploitation of our networks, the synergy between the 0600 and the 1700 communities must be … strengthened.

Notes

1. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, (August 2018), available at https://www.wired.com; and Joe Tidy, "Colonial Hack: How Did Cyber-Attackers Shut Off Pipeline?" *BBC News*, (May 2021), available at https://www.bbc.com.

2. *Hypr Security Encyclopedia*, s.v. "EternalBlue," available at https://www.hypr.com.

3. Staff, "Security update for Microsoft Windows SMB Server (4013389)," Microsoft, (March 2017), available at https://docs.microsoft.com.

4. Ellen Nakashima, "Russian Military Was Behind 'Notpetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, (January 2018), available at https://www.washingtonpost.com.

5. Staff, "Conflict in Ukraine," Council on Foreign Relations, (July 2021), available at https://microsites-live-backend.cfr.org.

6. William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Pasword," *Bloomberg*, (June 2021), available at https://www.bloomberg.com.

7. Emily McKeown, "What Is Multi-factor Authentication (MFA)?" *PingIdentity*, (September 2020), available at https://www.pingidentity.com.

8. Gen David H. Berger, "Preparing for the Future" Marine Corps Support to Joint Operations in Contested Littorals," *Military Review*, (May 2021), available at https://www.armyupress.army.mil.

9. Staff, "Glossary: Advanced Persistent Threat," National Institute of Standards and Technology, (n.d.), available at https://csrc.nist.gov.