Tactical Cyberspace Warfare

The road to follow

by Maj Byron Owen

>Maj Owen is an Infantry and Intelligence Officer. He deployed to combat numerous times as an infantry platoon and company commander. He commanded 1st Force Reconnaissance Company prior to his current assignment as the Commander, Combat Mission Team 1 at Marine Force Cyberspace Command.

Two automotive cybersecurity experts hacked a Jeep Grand Cherokee in 2015 and used its cellular network connection to remotely control the vehicle's brakes and acceleration. Chrysler quickly patched this vulnerability; however, this incident serves as a powerful reminder of what military cyberspace operators can do on the battlefield. Cyberspace warfare teams can potentially access, disrupt, or destroy any military system that is connected to the Internet. Most of these operations are currently executed remotely because of infrastructure and manpower requirements, but this may not be necessary or feasible in the future. Adversary threat systems will likely isolate their computer systems and operate inside closed looped networks that require physical proximity to access. Technological advances in computing, communications, and artificial intelligence will soon make it possible to link remote operators with forward deployed forces. The Marine Corps can complete the road to tactical cyberspace operations by deploying cyberspace operations capabilities forward with specialized equipment to connect the capabilities, infrastructure, and authorities that reside in Marine Forces Cyberspace Command (MARFORCYBER) with the tactical edge of the MAGTF.

Most military aircraft and vehicles do not currently connect to the Internet or a cellular network, but this will probably not be the case in the future.

It will soon be possible to link remote operators with forward deployed forces. *(Photo by PFC Kindo Go.)*

Most military aircraft and vehicles do not currently connect to the Internet or a cellular network, but this will probably not be the case in the future. The next generation of military equipment suites will likely reflect our society; everything will become much more digitized, networked, and interconnected. This will greatly increase situational awareness on the battlefield, accelerate targeting, and expedite fires deconfliction. It will also expose critical military systems to cyberspace exploitation and attack. Any networked device that connects to the Internet is potentially vulnerable to exploitation. Computers, run operating systems to perform their core functions, to include executing applications and peripheral devices. A skilled programmer can locate vulnerabilities in these systems and insert code, commonly referred to as malware, to direct the device to execute a command it was

not designed to do. For example, a malicious cyberactor can use malware to lock out a computer for a ransom payment, conduct corporate espionage, or steal crypto currency. A trained cyberwarrior can use similar techniques to neutralize networked air defense systems, degrade communications equipment, or disable multiple launch rocket systems. Cyberspace warfare will eventually revolutionize the battlefield in a way that has not been seen since the invention of the airplane.

It is no secret that cyberspace warfare specialists can potentially access and exploit any computer system that is connected to the Internet. This well-known vulnerability will encourage all combatants to isolate their tactical systems from the Internet. This does not mean, however, that they will be impenetrable to cyberintrusions. Researchers in Israel, for example, demonstrated techniques to access a closed computer network using radio signals in 2014,[1] and there are a number of ways to defeat WIFI encryption. That being said, all of these techniques require a significant amount of target-specific preparation and proximate access. This presents a complex obstacle on the road to tactical cyberspace operations. Strategic and operational cybertargets are not normally actioned in time sensitive environments. The same cannot be said for tactical targeting. Targets at the tactical level of war are often fleeting opportunities before a cyberteam can action them remotely. Pushing cyberspace warfare operators forward will not solve this problem either. In short, tactical cyber will likely require proximate access to attack closed enemy networks in the future, but it is not practical or feasible to deploy cyberspace warfare operators and their equipment forward to the battlefield.

It is easy to imagine Marines typing away enemy capabilities in the back of an armored vehicle, but this scenario will not be within reach any time soon. Cyberspace warfare operations require a significant amount of highly trained personnel and advanced technological infrastructure to conduct their operations. Our cyberforces must be able to clandestinely access target systems in a way that our adversaries cannot detect our intrusions, discover our malware, or expose the vulnerabilities we are exploiting. This requires a significant amount of software and physical hardware to accomplish. None of these systems are inexpensive or easily reproduced, and their large size and maintenance requirements make it impractical to deploy them forward. This is unlikely to change in the near future.

In addition to equipment limitations, there are also personnel shortfalls that stand in the way of tactical cyber. There are very few Marines who are qualified and certified to use this infrastructure to conduct offensive cyberspace operations. It takes over two years to train a cyberspace warfare specialist and their pipeline experiences and attrition rate that rivals Navy SEAL training. This manpower challenge is compounded because cyberspace warfare is a team sport with numerous highly specialized positions. No individual Marine can perform all the functions required to conduct an offensive cyberspace operation by himself. Imagine for a moment that cyberspace warfare specialists are competitive martial artists and cyberspace specialties are their techniques. It takes a significant amount of time to master a martial arts style, but proficiency in one form does not make someone effective in another. For example, a roundhouse kick is excellent technique to employ in a karate tournament, but it will likely get you disqualified in a judo match. Cyberspace specializations are very similar. Cyberspace weapons are designed to function against very specific combinations of hardware, software, and operating systems. A cybertechnique, commonly known as an exploit or cyberweapon, may work against a Windows device but may result in mission failure on a UNIX system. A cyberspace warfare team has to employ a bench of cyberspecialists to ensure that the right Marine is available to interact with a particular operating system. This is no easy feat given the extremely high attrition rates for each of the cyberspace warfare specialties.

There will never be enough cyberwarfare specialists to spread across the Marine Corps, but the answer to this puzzle is simple. Cyberspace is a global domain. The correct way to solve this problem is to remotely connect cyberspace warfare specialists to the battlefield rather than to forward deploy them. MARFORCYBER can deploy cyberspace operations liaison teams (COLTs) forward to advise MAGTF commanders on tactical cyberspace warfare capabilities and provide them with on-scene technical and tactical expertise. These liaison elements can also help MAGTF commanders communicate back to USCYBERCOM to request, deconflict, and coordinate tactical cyberspace fires. This small cell of planning experts can be task organized to meet mission requirements and include trained cyberspace mission commanders, cyberspace warfare specialists, and intelligence analysts. This will give commanders a comprehensive view of cyberspace warfare capabilities and limitations, and also inform them on the cyberthreats they need to defend themselves against. It is important to stress, that this team will be able to plan cyberfires for a MAGTF commander, but will not be able to execute any cyberattacks themselves. The COLTs will still need a digital tether back to MARFORCYBER. This linkage requires a technical solution that does not currently exist.

The Marine Corps must partner with industry to develop two technological components to bridge this gap. The first, a stable and robust data link, will not be difficult to produce.[2] The Department of Defense already posseses robust tactical SATCOM systems such as the HARRIS BGAN[3] and L3 PANTHER II[4] SATCOM radio antennas that should be able to create a suitable encrypted tunnel back to a CONUS based cyberspace warfare team. This technology will continue to evolve rapidly in the future and satellite communications will not limit remote cyberspace operations. The second component, a lightweight mobile device that can penetrate adversary networks, will be much more difficult to develop.

The technology theoretically exists to bring such a device to today's battlefield, but there are a number of factors that make it impractical to do so. A

cyberattack requires a specific pairing of a system vulnerability and a cyberweapon to be successful. Malware has to be designed to maneuver through the target's unique combination of computer hardware, software, firmware, operating system, networking devices and anti-virus defenses. This is an incredibly complex evolution and requires a significant amount of preparation. In other words, the DOD could probably field a cyberhowitzer in the very near future, but each cyberbullet would be an extremely precise round that would only work against a very specific target. Any deviance in the target system could require the cyberspace warfare team to reprogram the weapon system; however, this is not a timely process.

Technological advancements in computing and artificial intelligence will soon make this process much more agile. Artificial Intelligence will help automate some aspects of device exploitation to help locate vulnerabilities, quickly re-calibrate cyberweapons, and infiltrate networks. Quantum computing will make it possible to micronize this technology into portable devices with lightning fast processing power. The Marine Corps can put this technology into the hands of a reconnaissance team, or inside an unmanned aerial vehicle, to get the sensor in range of the target. All the team would need to do is turn on the sensor, establish a stable data connection back to MARFORCYBER over SATCOM, and the algorithm-enabled cyberwarriors will do the rest. This is not science fiction. Some of this technology exists; it just is not advanced enough to accomplish these tasks yet. It is only a matter of time, however, before it is ready to deploy onto the battlefield and the MAGTF provides an excellent platform to field this capability.

MARFORCYBER can leverage the Marine Corps' global presence to push tactical cyberspace warfare into the littorals and beyond. It takes a significant amount of time and effort to posture a cyberspace warfare team into a position to deliver a weapon to disable or disrupt an enemy system. The MEU provides U.S. Cyber Command with unparalleled access to adversary threat systems in semi-permissive environments as ships sail near adversary shores, move through contested areas during freedom of navigation operations, and deploy forces inland. The Marine Corps can extend this reach further with specially equipped UAVs or Marine reconnaissance teams. In the future, elements of the MAGTF will be able to reconnoiter adversary networks, develop a capability in the rear at MARFORCYBER, and inject it from a forward deployed platform. This enables U.S. Cyber Command to gain access to adversary systems during the shaping and deterring phases of an operation and be ready to execute cyberfires when hostilities commence.

Imagine a possible future of cyberspace warfare. A MEB steams toward an enemy coastline to conduct a joint forcible entry operation. They deploy a force reconnaissance team into the battlespace via high altitude high opening parachute infiltration to reconnoiter the beach landing site. The team discovers a networked enemy integrated air defense missile system. The team sets up their mobile cyberspace access device and scans the surface of the target network for vulnerabilities. The artificial intelligence enhanced sensor finds one and the force recon team reports this information back to the supporting arms coordination center aboard the USS *America* (LPD-17). The embarked COLT coordinates with MARFORCYBER to spin up a team to action the target. The reconnaissance team establishes a satellite data connection with the cyberspace warriors who then use this umbilical data-linkage to deploy an artificial intelligence enhanced cyberweapon into the enemy mobile integrated air defense missile system network. This smart malware clandestinely blinds all the air defense systems to all Marine Corps aircraft signatures. The adversary remains unaware of this intrusion until two days later when Marine Corps aircraft are flying overhead and all the anti-air devices are unable to target them.

This scenario may seem like science fiction today, but one day it will be our reality if we start pushing our procurement and development in this direction. The realities of the project objective management cycle means that the Marine Corps must use imagination and analysis to procure the equipment we need to defeat adversaries on tomorrow's battlefield. No one knows exactly what the future will look like, but we can make a good assessment if we channel equal parts of Ray Bradbury and Clausewitz. At some point in the near future, specially equipped reconnaissance teams, light armored reconnaissance vehicles, and unmanned aircraft will be able to extend a cyberspace warfare team's operational reach into any adversary's networked weapons system. Authorities may be a major sticking point today, but this will likely be resolved in the near future as policy makers and commanders become more comfortable with cyberspace operations. Russia and China both have robust cyberspace warfare programs and are rapidly developing artificial intelligence programs to enhance their military capabilities. The Marine Corps must invest in this technology and these concepts, or our Marines will find themselves at a severe technological disadvantage on tomorrow's battlefield.

Notes

1. K. Zetter, "How Hackers Can Use Radio Signals and Mobile Devices to Steal Protected Data," *Wired,* (Online: November 2014), available at https://www.wired.com.

2. This of course does not account for electronic warfare, which is a very real threat to this concept of cyberspace operations but outside the scope of this article.

3. Harris Corporation, "Harris RF 7800B BGAN Terminal System." *Harris Radio*, available at https://www.harris.com.

4. Global Communications, "Manpack-Panther II," *Global Communications Systems* (Online), available at http://www.globalcoms.com.