Cyber Small Arms

Enable training for maneuver commanders

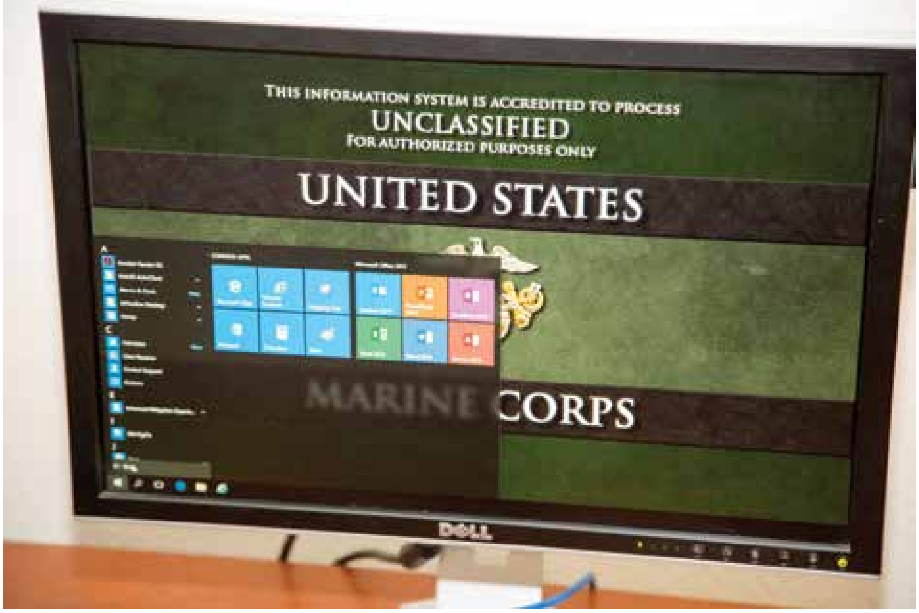
by Capt Kurt D. Iversen, USAF

>*Capt Iversen is a USAF 17D, Network Operations Officer, currently assigned to the Office of the Deputy Chief Information Officer, USCYBERCOM/J9. He is a 2019 graduate of Expeditionary Warfare School and has worked in air defense networking, cyber defense, and various special duties. The opinions expressed in this article are his own and not endorsed by his Service or command.*

The *Marine Corps Operating Concept* calls for the MAGTF to fight through "combined arms in all domains," including the cyber domain, and this requires developing organic cyber capabilities.[1] Meanwhile, maneuver warfare describes tempo as a way to seize initiative and generate combat power.[2] To do this, the Marine Corps should develop cyber small arms that allow tactical commanders to integrate limited offensive cyberspace capabilities into operations.

Cyberspace operations assigns offensive cyber operations (OCO) to the commander of United States Cyber Command (USCYBERCOM), who "conduct[s] military [cyberspace operations] external to the [Department of Defense Information Network]."[3] Meanwhile, other combatant commands (COCOMs) only "secure, operate, and defend" their parts of the network.[4] Thus, USCYBERCOM forces conduct OCO in support of other COCOMs' requirements.[5] This requires a great deal of coordination. The commander of Central Command recently argued for "broader authorities that are more responsive than current bureaucratic processes."[6] The status quo puts tactical commanders in a dilemma, forced either to give up the benefits of OCO or to forfeit tempo to coordinate up to their COCOM and over to USCYBERCOM. Allowing tactical commanders the authority and capability to conduct limited OCO will resolve this dilemma.

To provide OCO in support of tactical units, a new class of tools—cyber small arms—is needed. By analogy, conventional small arms can inflict personnel casualties but cannot destroy armored vehicles. Likewise, cyber small arms will degrade or disrupt the enemy's use of cyberspace within the physical area of operations of the employing unit by targeting vulnerable enemy nodes within that area, but cyber small arms will not succeed against every hardened node.



This information system is accredited to process
UNCLASSIFIED
For authorized purposes only
UNITED STATES
MARINE CORPS
DELL

Is there a known vulnerability? *(Photo by Keith Hayes.)*

The effects of cyber small arms will be limited in three ways: technical design, procedures for use, and rules of engagement (ROE) governing employment. Cyber small arms will be designed without using secret vulnerabilities in common programs or self-replicating code that spreads beyond the target.[7] Operator procedures, such as using intelligence to confirm that a targeted node is part of the enemy command post, will ensure that the weapons are used in a controlled manner. ROE will define permitted targets, such as excluding civilian cyberspace infrastructure to limit negative higher order effects. These limitations allow employment to be pushed to tactical-level commanders, shortening the decision cycle and reclaiming tempo while benefiting from OCO.

For example, a cyber small arm targeting a known vulnerability would only succeed against enemy systems that were missing a patch, but disrupting even a single computer could distract the enemy (focusing attention on the cyberattack) or erode confidence in their system (causing doubt about other computers and shifting to predigital methods).[8] By targeting a known vulnerability, a cyber small arm is less expensive to develop and does not reveal a new capability either for patching or for the enemy and third parties to exploit when used.

To understand why the current doctrine is so restrictive, it is helpful to consider an example of successful OCO. The worm Stuxnet sabotaged centrifuges enriching uranium in an Iranian nuclear facility.[9] To spread between computers, Stuxnet used technical capabilities including five zero-day vulnerabilities.[10] A zero-day is a vulnerability in a program that lets an attacker gain access to the system, but that is unknown to the program's developer. This means that there is no corrective patch to close the vulnerability nor is there a fingerprint for anti-virus programs to detect the attack.[11] Because zero-days allow access to any computer running the program, they are valuable for espionage or criminal organizations seeking to exploit computers, with one cybersecurity company offering up to $1.5 million dollars for a zero-day exploit.[12] Once a zero-day attack is detected, the program developer may develop and release a corrective patch to secure the program, and anti-virus companies can add the attack's fingerprint to their products.[13] These responses take time, leaving a window between detection and patching during which other hackers can exploit the vulnerability.[14] Using a zero-day not only means that the vulnerability may be fixed but also that enemy or criminal organizations may use the same zero-day in the near term.[15]

A zero-day is a vulnerability in a program that lets an attacker gain access ...

Stuxnet spread globally, but it did not cause widespread damage.[16] It looked for the combination of a certain controller model connected to between 1 and 186 centrifuges using two specific brands of power converters and spinning within a specified frequency range.[17] These checks within the program assured that it would only cause damage at the Natanz enrichment facility even though it infected many other computers.

Using cyber small arms provides the commander a new way to engage enemy targets. *(Photo by Cpl Garrett White.)*

Stuxnet exemplifies why offensive cyberspace capabilities are tightly controlled. Impeding a state's nuclear program and that state's response, if discovered, are strategic concerns. Because Stuxnet spread so broadly, if it had accidentally damaged all infected systems, it would have impacted industrial processes globally. Once Stuxnet was discovered and analyzed, it ceased to be capable: the vulnerabilities were patched. Finally, breaking centrifuges increased the likelihood that the Iranians would realize that their network was infected, triggering a response that would wipe out access to the facility.

Programs like Stuxnet are strategic assets, but not all offensive cyber capabilities should be controlled the same way. Zero-days are highly capable tools that may stop working once used, and their use risks teaching the enemy or third parties how to exploit the same vulnerability until it is patched. These properties mean that their use must be centrally coordinated to avoid wasting a capability that is planned for another target or held in reserve.[18] Not all cyberattacks require zero-days though.[19] Cyber small arms can attack soft targets through older vulnerabilities.

The WannaCry cyberattack demonstrated how effective it can be to target a vulnerability even after a fix is publicly available. WannaCry was designed to spread widely and extort affected computer users, and it spread to over 200,000 computers in 150 countries within a day of its release.[20] Microsoft not only knew about the vulnerability that WannaCry targeted, but they had released a patch for the vulnerability months before the attack began.[21] WannaCry could only infect systems that had not installed the security patch, but it still found 200,000 such systems.

There are several objections to allowing a tactical commander to employ OCO: cyber arms are inherently strategic, the technical capability is risked each time it is employed, the risk of collateral damage is too high, and the tactical commander lacks the perspective to assess the intelligence gains and losses involved in the operation.

Some cyber arms do qualify as strategic weapons. When deciding to use

Stuxnet, the potential for Iran to detect and retaliate for the attack had to be weighted against the benefit of destroying the centrifuges. The easiest way to handle such strategic considerations for cyber small arms is through ROE. At a minimum, these rules will specify when cyber small arms may be employed (such as with combat operations, not during pressure campaigns) and what targets they may engage (such as enemy tactical nodes but not the enemy commander's bank account).

Because cyber small arms do not employ zero-days, the technical loss if an attack is detected is minimal. The enemy will not learn about a new vulnerability to use against friendly forces. The enemy could realize what vulnerability a cyber small arm targeted and patch it to prevent the same small arm from working in the future, but because cyber small arms use publicly known vulnerabilities, they are much less expensive to develop.[22] This means that a unit could be equipped with multiple cyber small arms targeting different vulnerabilities, and they would switch between them as the enemy responded to attacks.

Stuxnet avoided collateral damage by ensuring that it would only execute its payload against the centrifuge assembly at Natanz, which was required because the program itself was designed to spread widely.[23] With cyber small arms, the risk of collateral damage can be managed through a combination of weapon design (avoiding self-spreading code), operator procedure (using intelligence to target specific enemy military internet protocol addresses), and ROE (excluding nodes which are used by both civilian and enemy military traffic).

The final objection is that tactical commanders do not have the perspective to evaluate the loss of future intelligence because of cyber small arms attacks (if an enemy node goes off-line, it cannot be exploited by national intelligence agencies). Restricting cyber small arms to only target nodes physically within the tactical area of operations accounts for this. Commanders already have the authority to engage military targets within this area using kinetic means (e.g., an artillery strike against an enemy command post), which means that they already need to evaluate the loss of future intelligence (if the command post is destroyed, it cannot be hacked). Providing the commander with cyber small arms allows a new means to engage enemy targets, but because it does not provide additional targets, it does not require new considerations for the loss of future intelligence.

...the risk of collateral damage can be managed ...

The Marine Corps should develop cyber small arms to integrate organic OCO into the MAGTF. This article considered the technical, procedural, and engagement requirements for allowing tactical commanders to employ cyber small arms in open conflict. There are multiple areas for additional development on this topic. Cyber small arms could be used in developing partner capability because they do not use zero-days. As acknowledged capabilities, they could deter malicious cyber activity as called for in the National Cyber Strategy.[24] Additionally, they will both require and enable cyber capability education for tactical maneuver commanders.

Notes

1. Headquarters Marine Corps, *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century,* (Washington, DC: September 2016).

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

3. Department of Defense, *Joint Publication 3-12, Cyberspace Operations*, (Washington, DC: June 2018).

4. Ibid.

5. Ibid.

6. Joseph Votel, David J. Julazadeh, and Weilun Lin, "Operationalizing the Information Environment: Lessons Learned from Cyber Integration in the USCENTCOM AOR," *The Cyber Defense Review,* (West Point, NY: Army Cyber Institute, Fall 2018).

7. Martin Libicki, *Cyberspace in Peace and War,* (Annapolis, MD: Naval Institute Press, 2016).

8. Ibid.

9. Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,* (New York, NY: Crown Publishers, 2014). See also *Cyberspace in Peace and War.*

10. Ibid.

11. Ibid.

12. Ibid. See also *Cyberspace in Peace and War.* Additional information is available at the Zerodium website available at https://www.zerodium.com.

13. *Countdown to Zero Day.*

14. Ellen Nakashima, "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did," *The Washington Post*, (Washington, DC: May 2017).

15. Ibid.

16. *Countdown to Zero Day.*

17. Ibid.

18. *Cyberspace in Peace and War.*

19. Ibid.

20. Elizabeth Piper, "Cyber Attack Hits 200,000 in at Least 150 Countries: Europol," *Reuters*, (May 2017), available at https://www.reuters.com. See also Lily Hay Newman, "The Ransomware Meltdown Experts Warned About Is Here," *Wired*, (May 2017), available at https://www.wired.com.

21. Ibid.

22. *Cyberspace in Peace and War.*

23. Ibid.

24. The White House, *National Cyber Strategy of the United States of America,* (Washington, DC: 2018).

UB✣MC