Putting the Meat on the Bones

Why we need cyber operational graphics

by Maj Paul L. Stokes (Ret)

South China Sea, 2025

D+16, the tension in the MEB landing force operations center was at a fever pitch as Col Crusher, the MEB G-3 (Operations), LtCol Sparks, the MEB Cyberspace/Electronic Fire Support Coordinator (aka G-6 Communications), and the rest of the principal staff looked over a map of the MEB amphibious objective area (AOA).[1] *Col Crusher was old school and insisted upon acetate overlays that, when placed on top of each other, graphically depicted how each element of the MEB—to include kinetic and cyber fires—supported the seizure of MEB Objective Bravo, the second largest island in an archipelago of man-made islands that the enemy was using to blockade international commerce.*

In a clipped, concise tone, LtCol Sparks explained his cyberspace/electronic fire support (Cyber/EFS) overlay to include key terrain, zones of control, and both offensive and defensive actions. As the G-6 answered questions from the staff, it reinforced Col Crusher's conviction that he had done the right thing by going back to the basics and insisting that the MEB use operational graphics in all of their products—including Cyber/Electronic Fires. Not only do they give the MEB staff and ground, air, and logistics command element commanders a common language but they also put the meat on the bones of these seemingly nebulous yet vital command and control (C2)/operational cyber capabilities. They mitigate the effects of the fog of war by conveying the MEB commander's intent in clear, unequivocal terms that any Marine will understand.

>Maj Stokes retired in August 2006 after 31 years of active-duty service. A former Gunnery Sergeant and Chief Warrant Officer 3, he has served in a variety of Leadership and Communications billets from the Team to Theater Levels. Maj Stokes has served as the Marine Corps Communication-Electronics School's Operations Officer, Deputy Operations Officer, Future Operations/Plans Officer since January 2007.

U.S. Marine updating map overlays in a landing force operations center. ***(Photo source: dvidshub.net.)***

The Primitive State of Cyber Operational Graphics[2]

Presently, all elements of the MAGTF (-) Cyber/ EFS units have specialized sets of symbols that convey information/understanding more quickly than verbal/text orders.[3] Symbols have been part of military operations for a millennium, which is why in MAGTF operations it is crucial to have a set of common cyber operational graphics *to put the meat on the bones*.[4] In 2009, the DOD established the cyberspace warfighting domain, but our Cyber/EFS units still lack a coherent set of symbols that allow them to convey the intricacies of cyber warfare to both the Marine Corps and the joint warfighting community.[5] This inability to easily express operational concepts inhibits the identification of cyber key terrain, development of cyber tactics and strategies, and execution of C2.

DOD has a joint standard for military graphics, *Joint Military Symbology,* which provides a basic set of cyber symbols.[6] However, these symbols display cyber effects and network nodes only in the physical domain and are unable to portray cyber warfare in the logical and personal layers of cyberspace. In response, the Institute for Defense Analyses (IDA) developed a symbol set that is both compliant with DOD standards and capable of displaying the nuances of cyber warfare in support of MAGTF and joint operations.[7]

The primitive state of cyber operational graphics and the lack of effective communication between the cyber and physical warfighting domains deemphasizes the application of the principles of war in cyber operations. This increases the likelihood that our Marines will accept dangerous risks because they have little concept of what is really happening on their networks. Therefore, our cyber/EFS units must transform from being predominantly specialists trained and organized to accomplish specific missions into *cyber bases of fire*[8] that are fully capable of planning and executing offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD infrastructure operations (DODIN Ops).[9]

It is no longer just the Internet; it is the battlefield and adopting cyber symbols will give our Cyber/EFS Marines insight into the parallel activities performed in other domains.

Cyber/EFS units do not lack for symbols—network diagrams are ubiquitous—but these symbols do not conform to MAGTF/joint doctrine. A firewall needs to be recognized as a fortification. A honeypot *is* an ambush site or a delaying obstacle in cyberspace.[10] Scanning *is* reconnaissance, and networks *are* areas of responsibility. Cybersecurity service providers and network operations centers are cyber protection teams, companies, battalions, brigades, or higher. Offensive cyber mission teams conduct raids, strike targets, and execute active defense missions using preemptive attacks. It is no longer just the Internet; it is the battlefield and adopting cyber symbols will give our Cyber/EFS Marines insight into the parallel activities performed in other domains.

By standardizing these symbols, a MAGTF commander will be able to understand what is happening on the cyber front. He may be unclear on how it got through the firewall, but he will intuitively understand red arrows bypassing his fortifications and driving deep into his cyber key terrain.[11] Soon he will learn to discern which cyber-related decisions are risky and which are not. The cyber battle, currently fought apart from the land-sea-air battle, must and will be integrated into MAGTF operations.[12]

Terrain Graphics[13]

Terrain is the fundamental venue for military action, in cyberspace as well as in the land, sea, and air domains. *JP 3-12, Cyberspace Operations,* divides the cyberspace domain into three layers: the physical, logical, and persona.[14] The physical layer is the hardware, located in the physical domain, on which the other two layers exist. The physical layer is not cyberspace terrain itself. Symbols for physical equipment already exist in *Joint Military Symbology*.[15] The logical layer is where cyber terrain exists, and the primary cyber terrain feature is the network, a collection of devices that implement applications, services, and data storage. It is often governed by Internet protocol ports and addresses accessed through a router. Networks are the cyber equivalent to areas of operations in the physical domain, and their existence is provisioned by the assigned MAGTF domain accreditation authority, which issues policy guidance/exercises C2 over subordinate units within the mission category of DODIN Ops. When protected by a firewall and monitored by intrusion detection services at ingress points, a network becomes fortified and has a sensor line; when guarded by cybersecurity service providers, cyber protection teams, and unit cyber defenders, it is analogous to the most common C2 area designation: the operational area (OA).[16]

Individual networks can be depicted with a unique boundary line that represents the extent of the Internet protocol address space within it (see Figure 1). For clarity, the MAGTF G-6 would only depict the number of devices necessary to describe the planned/observed cyber operations or to convey an understanding of the nature of the terrain. For instance, if only one device out of hundreds on the network is attacked, we can show that device alongside a half-dozen others, often with a note that the small number of devices depicted is representative of many more.[17]

Color-coded boundaries for each network can also be employed to enable a quick understanding of the terrain because relatively few unique networks are typically required to depict a cyberspace battle and because alphanumeric des-

ignations defining the boundary with adjacent areas, as is typically done in the physical domain, make no sense. However, a unique alphanumeric designation for a network could certainly be used as a label to identify its boundary.[18]

Cyber terrain is unique because it is completely manmade, and distance is measured in "hops" between computers rather than in kilometers—time and space have different relationships and affect operational decisions differently than they do in the physical domain. Cyber terrain is also changeable on short timescales. If we do not like how the enemy is using our terrain, we can simply change it by disconnecting from the network or shutting down vulnerable devices. Because of the nature of cyberspace, the distance between, and the relative positioning of, unique independent networks have little meaning in operational graphics depictions. However, the relationships between networks, such as where one is a subdomain of another, *are* important, so consequently, we can depict subdomains as existing completely within their parent networks.[19]

Devices in cyber generally function simultaneously as terrain features on which forces maneuver and as installations (which provide C2, offensive, defensive, surveillance, supply, transportation, or other warfighting functions); thus, they have no clear analogies in the physical domain. But it is possible to adopt common network diagram symbols in simplified form depicting an individual workstation or client as a square and a server as a circle. However, two specialized devices (and the functions they perform) that are nearly always present in cyber battles would be assigned unique symbols, the firewall: represented as a fortification; and the intrusion detection equipment/services: represented as a string of sensors.[20]

Similar to its physical counterpart, a cyber OA can be secured, contested, or captured. However, unlike in the physical domains, where control is often contested but never truly shared during typical combat operations, cyber OAs can experience dual control when an adversary has gained credentials that provide access to the terrain—servers, applications, and data storage—within the OA without the defenders being aware of the compromise. This situation is analogous to insurgency operations, wherein a guerrilla unit operates clandestinely in the shadow of the occupying unit. Actual capture of a complete cyber OA is rare but can happen when the elements of the physical layer fall into enemy hands surreptitiously and the defenders do not realize that they ought to sever the connections between the OA and the rest of the network—a prime mission for special forces. Red shading represents devices that have fallen under enemy control in some way. In some instances, red shading may be used to represent enemy control over an entire network. [21]

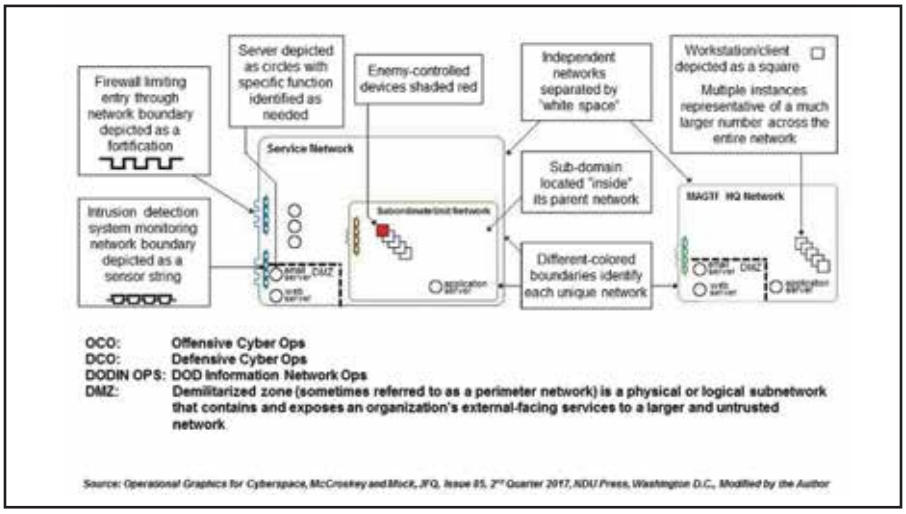


Figure 1. Cyberspace terrain description: networks and common features. *(Figure provided by author.)*

Persona and Credential Graphics[22]

The persona layer is the means by which personnel/units operate in cyberspace**.** The cyber persona layer requires a higher level of abstraction because Marines do not exist in cyberspace but do have accounts and their associated credentials, i.e., usernames, passwords, common access cards, and personal identification numbers, that serve as the primary means to plan and execute administrative actions, domain control, user activity, printer access, or any number of function-related activities. The tendency is to think of accounts as people, whereas it is more logical, from a cyber perspective, to think of accounts in terms of the equipment used by Marines existing in the physical domains. For example, in the air domain, a pilot (the operator) uses an F-35B (a piece of equipment) to conduct a variety of air superiority missions; similarly, a network user account is a piece of cyber equipment that allows the operator to conduct email, use a Microsoft Office application, or communicate with other accounts. The difference is that the F-35B pilot is physically paired with his aircraft in the air domain, whereas the cyber operator resides in the physical domain (where the physical layer of cyber exits) and conducts his mission in the cyberspace domain via the logical/persona layers, looking in from the outside. MAGTF units thus have a foot in two domains: the Marines/physical layer hardware in one domain, and the mixed types of accounts, credentials, cyber actions, and missions in another.[23]

Credentials are the keys to cyber equipment and associated accesses/privileges. Enemy control of a user-level account is damaging because it allows him to traverse the operations area in the guise of a friendly operator. An enemy who gains credentialed access to a domain administrator account can use the privileges associated with this account to control all the key terrain—accounts, servers, data, and applications—in that operations area. Different key symbols reinforce this

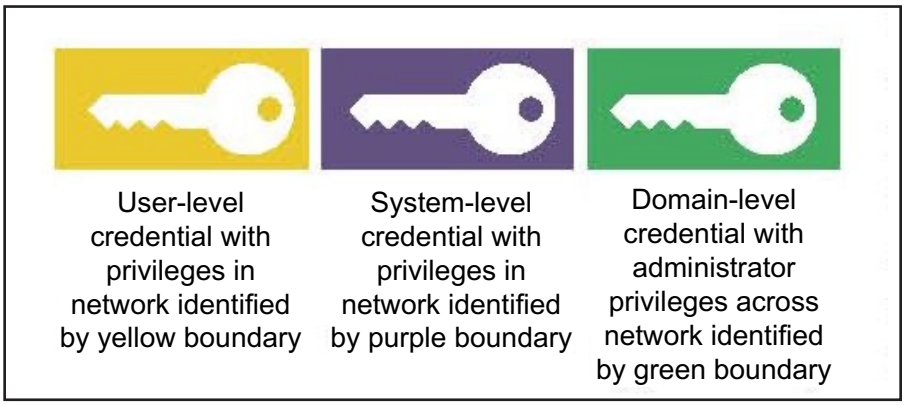
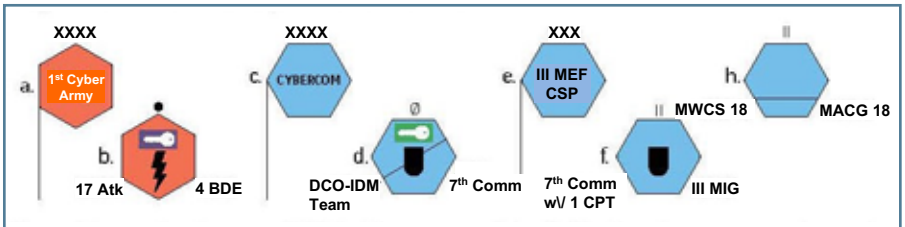


Figure 2. Notional cyber credential icons. *(Figure provided by author.)*



Key: a. Enemy headquarters (HQ); b. Enemy squad-level OCO unit with captured system admin credentials; c. US Cyber Command HQ; d. Friendly DCO unit with reconnaissance capabilities that has been granted domain administration credentials/authorities; e. Friendly cyber service provider HQ; f. Friending DCO unit; d. Friendly DODIN Ops cyber unit.

OCO:	Offensive Cyber Ops	MFCY:	Marine Forces Cyber Command Warfare Group
DCO:	Defensive Cyber Ops	MEF:	Marine Expeditionary Force
DODIN OPS:	DOD Information Network Op	MIG:	MEF Information Group
CSP:	Cyber Service Provider	MACG:	Marine Air Control Group
CPT:	Cyber Protection Team	MWCS:	Marine Wing Communication Squadron
CYBERCOM:	U.S. Cyber Command	DCO-IDM:	Defensive Cyber Operations – Individual Protective Measures

Source: Operational Graphics for Cyberspace, McCroskey and Mock, JFQ, Issue 85, 2nd Quarter 2017, NDU Press, Washington D.C., Modified by the Author

Figure 3. Notional cyber unit icons. *(Figure provided by author.)*

point: yellow for user-level, purple for system-level, and green for domain-level privileges. A colored border around the key indicates the domain or network to which the privileges pertain.[24] (see Figure 2.)

Unit Graphics[25]

Joint Military Symbology prescribes the use of specific frames for icon-based symbols to depict the identities of units operating in the land, sea, air, space, and sub-surface physical domains. It does not prescribe a unique frame to identify units when depicting operations solely in cyberspace (i.e., logical and persona layers).[26]

We can adopt a regular hexagonal frame to depict units in cyberspace to include standard shading/rotation conventions for friendly, neutral, hostile, civilian, and unknown standard identities (See Figure 3).[27]

Cyber icons must represent the unique nature of Marine cyber/EFS units. This is why our symbols should be based on the three general mission categories: OCO, DCO, or DODIN Ops. This is why a lightning bolt identifies OCO units, a shield icon identifies DCO units, and existing support unit symbols identify DODIN Ops units.[28]

Detection is critical to successful cyber operation, and individual cyber/EFS units (i.e., defensive cyber operations/individual defensive measure [DCO/IDM] companies)[29] are assigned "detect" as a priority mission and are specially equipped and trained to execute it. Marine units performing the detect mission are depicted with a diagonal slash across the frame, similar to the use of a slash to denote reconnaissance capabilities in the physical domains.[30] Cyber/EFS units are identified by the echelon command level to which they belong, just as units in the physical domain, but one should take care when inferring echelon-level missions, capabilities, and resources since these are not directly comparable to units in the physical domain. Physical domain units at the same echelon level can exhibit substantial variation in their numbers of assigned personnel and equipment, as well as in their capabilities and "reach" (i.e., an infantry battalion may have 800 Marines assigned and fight on a front of perhaps 5 miles, while a fighter squadron may have 150 Marines/12 aircraft assigned and fight within a 500-mile radius of its base).[31]

The variation between cyber and physical units within the same echelon, however, tends to be even greater. For example, a DCO/IDM company may be responsible for *global* detection and response efforts for an entire regional network. Additionally, there will be fewer units at any given echelon within the cyber force structure, allowing the adoption of the existing echelon representation (used primarily in representing land force units) and applying it using the official designations of cyber/EFS units with U.S. Cyber Command as the top echelon.[32]

Mission Graphics[33]

Although some graphic control measures used in the land domain (such as phase lines, assembly areas, fire support coordination measures, and checkpoints) may not be useful in describing operations in cyberspace, others can be readily adapted for the purposes of planning and maintaining situational awareness. In addition to the potential utility of adapting general offensive graphics (axis of advance, direction of attack), general defensive graphics (fortified line for firewall, sensor outpost for monitored intrusion detection device/system), and supply graphics (main supply routes or lines

Table. Adaptation of Tactical Task Graphics to Cyberspace

Tactical Task	Operational Graphic	Doctrinal Description (MIL-STD-2525D)	Potential Use in Describing Cyberspace Operations
Actions by Friendly Force			
Attack by Fire		The use of direct fires, supported by indirect fires, To engage an enemy force without closing with the enemy to destroy, suppress, fix or deceive that enemy	Overt actions where an origination (or interim relay) point can be determined, such as distributed denial-of-service attacks, broad intrusive scans, where these actions create the intended effect on the target.
Breach		Break through or establish a passage through an enemy defense, obstacle, minefield, or fortification.	Noncredential-based access (penetration through a firewall, using an exploit or hacking tradecraft).
Bypass		Maneuver around an obstacle, position, or enemy force to maintain momentum of the operation while deliberately avoiding combat with an enemy force.	Credential-based access (use captured credentials for login).
Clear		Remove all enemy forces and eliminate organized resistance within an assigned area.	Comprehensive scans and forensics, removing all malware and enemy points of presence and external connections.
Control	N/A	Maintain physical influence over a specified area to prevent its use by an enemy or to create conditions necessary for successful friendly operations.	Standard cybersecurity mission to protect a domain, typically assigned to a cyber security provider (CSP).
Counter-reconnaissance (Screen)		Provide early warning to the protected force.	Detection activities on a boundary or domain.
Counter-reconnaissance (Guard)		Protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. Units conducting a guard mission cannot operate independently because they relay upon fires and combat support assets of the main body.	Domain-wide detection and hunt-type activities by a Cyber Protection Team (CPT) or local defensive unit, augmenting the capabilities of a CSP.
Counter-reconnaissance (Cover)		Protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body.	Domain-wide detection, hunt, and restricting of defensive boundary controls by a CSP.
Exfiltrate	 (No symbol exists. Symbol shows the flow of exfiltrated data, a substantial deviation from the existing definition of this task.)	Remove Marines or units from areas under enemy control by stealth, deception, surprise, or clandestine means.	Movement of data from its original location to a location under enemy control, typically by means of stealth, deception, surprise, or clandestine means.
Occupy		Move a friendly force into an area so that it can control that area. Both the force's movement to and occupation if the are occur without enemy opposition.	Deployment of a Cyber Protection Team (CPT) to a domain in advance of a suspected enemy activity.
Retain		Ensure that a terrain feature controlled by a friendly force remains free of enemy occupation or use.	Defense of a network device or domain to prevent any enemy access.
Secure		Prevent a unit, facility or geographical location from being damaged or destroyed as a result of enemy action.	Defense of a network device or domain to prevent an enemy from making any changes to data or functionality.
Seize		Take possession of a designated area by using overwhelming force.	Gain control of a device, network, data, or credentials. In cyperspace, two opposing forces *may* have simultaneous control of any or all of these assets.
Support by fire		A maneuver force moves to a position where it can engage the enemy by direct fire in support of another maneuver force.	Overt action where an origination (or interim relay) point can be determined, such as distributed denial-of-service attacks, broad intrusive scans, and where these actions are designed to set the conditions for success for the primary attack actions.

Source: Operational Graphics for Cyberspace, McCroskey and Mock, JFQ, Issue 85, 2nd Quarter 2017, NDU Press, Washington D.C., Modified by the Author

Table 1. Cyberspace actions by friendly force. *(Table provided by author.)*

Table. Adaptation of Tactical Task Graphics to Cyberspace

Tactical Task	Operational Graphic	Doctrinal Description (MIL-STD-2525D)	Potential Use in Describing Cyberspace Operations
Effects on Enemy Force			
Block		Deny the enemy access to an area or prevent the enemy's advance in a direction or along an avenue of approach. Also an obstacle effect that integrates fire planning and obstacle efforts to stop an attacker along a specific avenue of approach or prevent the attacking unit from passing through an engagement area.	Use or modification of blacklists, whitelists, access control lists, routing policies, credentials (username-password pairs, or machine-issued), or filters on firewalls, domain name servers, domain controllers, Web servers, Email servers, or others to prohibit or terminate access based on specific criteria.
Canalize		Restrict enemy movement to a narrow zone by exploiting terrain coupled with the use of obstacles fires, or friendly maneuver.	Use of routing policies, honeypots/honeyports/ honeynets, or other defensive techniques to direct potential adversary traffic to desired network locations.
Contain		Stop, hold, or surround enemy forces or to cause them to center their activity on a given front and prevent them from withdrawing any part of their forces for use elsewhere.	Not strictly possible in cyberspace, since forces exist as a function of effort being expended. However, could be used to indicate quarantine of malware or emails.
Destroy		Physically render an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.	Deleting all files from a server, flashing basic input-output system or firmware, or causing physical damage to industrial control systems.
Disrupt		Integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt the enemy's timetable, or cause enemy forces to commit prematurely or attack in a piecemeal fashion.	Interrupting connections periodically, enforcing time limits on sessions, or actions that require an enemy to repeat previous steps, upset an enemy's tempo, interrupt the enemy's timetable, or cause the enemy's efforts to proceed in a piecemeal fashion.
Fix		Prevent the enemy force from moving any part of that force from a specific location for a specific period.	Not strictly possible in cyberspace, since forces exist as a function of effort being expended, but used to indicate actions that require an enemy to focus effort to restore function (for example, reboot a domain controller or data server following an induced system crash); to expend much greater effort than planned to obtain an objective (for example, consuming attacker resources using a realistic honeynet); or refrain from using capabilities for fear of detection (for example, refrain from activating implants because of increased random scans for active malware).
Interdict		Prevent, disrupt, or delay the enemy's use of an area or route.	Denial-of-network (data transport) service, or limiting access to services.
Isolate		Requires a unit to seal off both - physically and psychologically – an enemy from sources of support, deny the enemy freedom of movement, and prevent the isolated enemy force from having contact with other enemy forces.	Removal of a device infected with malware from the network, moving a phishing email from the server to a forensics sandbox.
Neutralize		Render enemy personnel or material incapable of interfering with a particular operation.	Any action taken against another cyberspace *unit* that prevents it from using its offensive or defensive capabilities (for example, interrupt the sensor feeds from a target domain to the responsible cyber defense unit).

Note: 1. A ***honeypot / honeyport / honeynet*** is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.

2. A ***sandbox*** is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system.
3. ***Phishing*** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (i.e., email, web link, or web post).

Source: Operational Graphics for Cyberspace, McCroskey and Mock, JFQ, Issue 85, 2nd Quarter 2017, NDU Press, Washington D.C., Modified by the Author

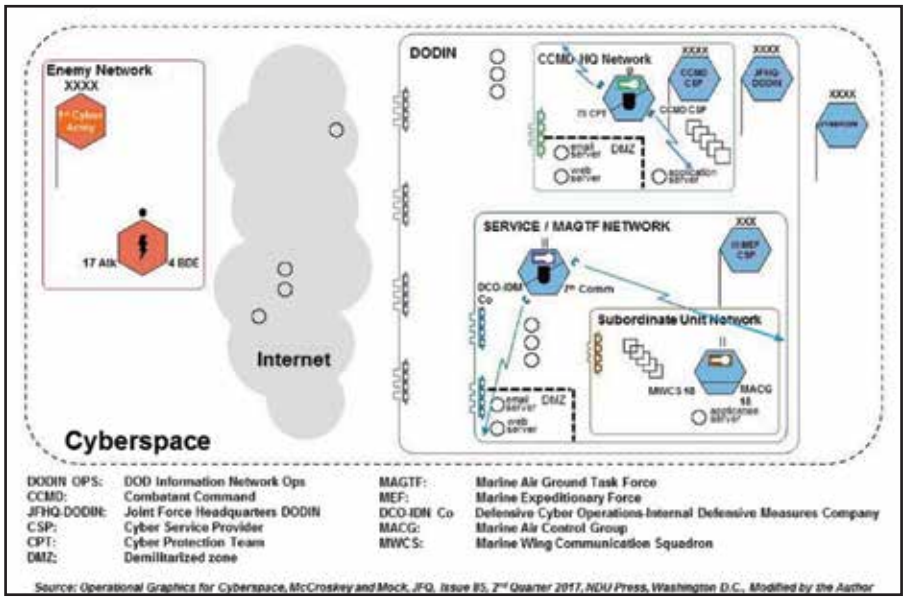
Table 2. Cyberspace effect on enemy force. *(Table provided by author.)*

of communications for data flows), the traditional definitions of tactical mission graphics can be modified to depict actions in cyberspace. Potential adaptations of these graphics to cyberspace are provided in Tables 1 and 2.

Putting It All Together

These basic building blocks allow the portrayal of cyber battles in a straightforward manner and present the required action in a familiar format. The symbol set is still small—units, terrain, C2, attack vectors—but capable of providing those insights a MAGTF commander needs for situational awareness of the operations area. Marine operating force G-6s already understand why firewalls and sensors are ineffective once the enemy has gained credentials through phishing and poor password protection; battle maps with an attack arrow showing an enemy task force masquerading as friendlies and penetrating a fortification to pass undetected through sensors provide the MAGTF commander with an understanding—an enormous red flag signaling risk to his mission—that has been missing from the cyber portion of MAGTF/joint warfighting.[34]

Figures 4, 5, and 6, (using the graphics in Tables 1 and 2), depict the progression of a notional battle in cyberspace, from the initial assignment of defensive forces to their areas of responsibility, followed by the attacker's preparatory reconnaissance operations, and culmi-



Source: Operational Graphics for Cyberspace, McCroskey and Mock, JFQ, Issue 85, 2nd Quarter 2017, NDU Press, Washington D.C., Modified by the Author

Figure 4. Notional cyberspace terrain showing boundaries, units, and defensive tasks. *(Figure provided by author.)*

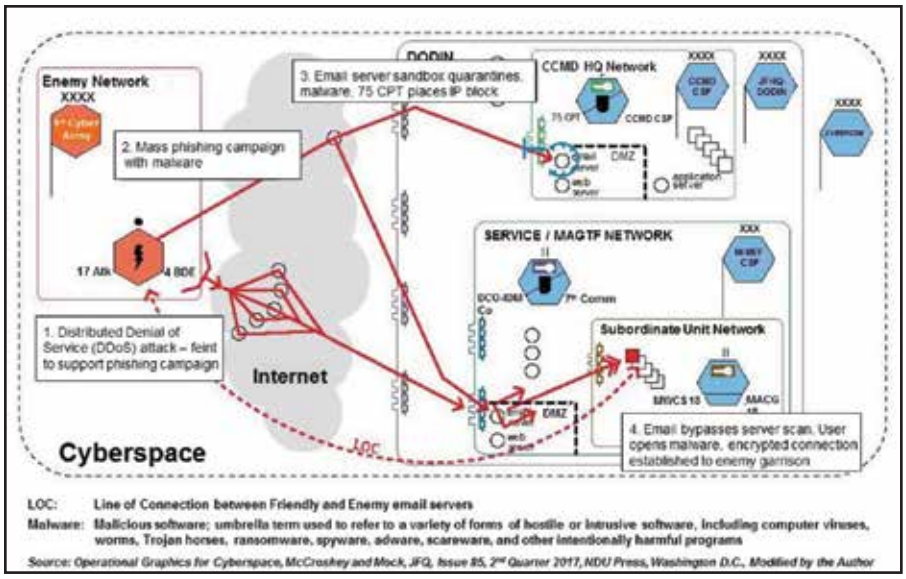


Figure 5.Sequential actions in the initial enemy assault; a feint, blocked phishing attack, successful bypass of defenses that gains control of friendly cyberspace terrain. ***(Figure provided by author.)***

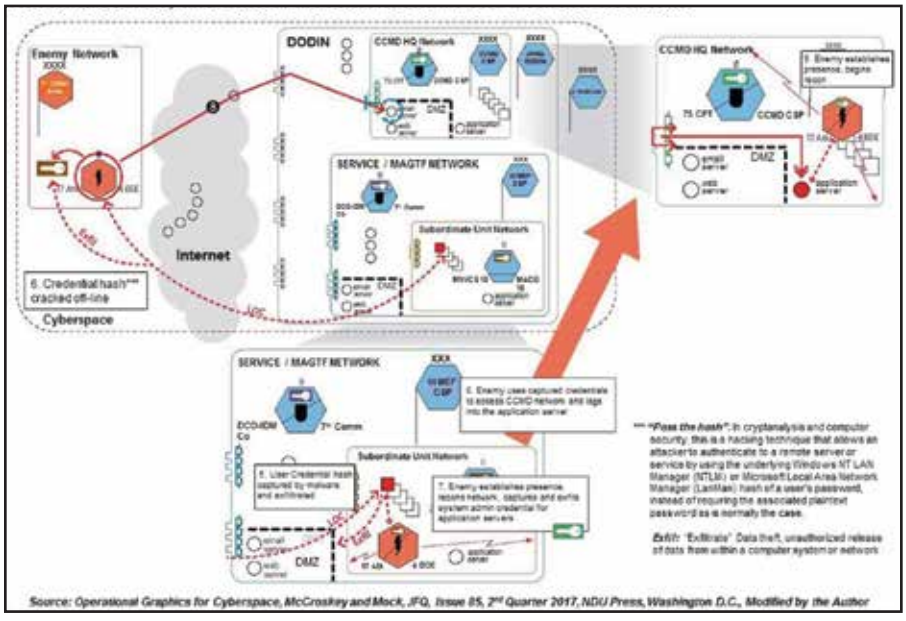


Figure 6. Sequential enemy actions on friendly cyberspace terrain; seizing of credentials, reconnaissance, and lateral movement within and between networks. ***(Figure provided by author.)***

nating in the penetration of defenses and the attacker occupying defended territory and postured to conduct follow-on operations. This validates IDA's assessment that by adopting common cyberspace symbols—based on proven doctrine—cyber operational graphics will earn their place as an equal amongst terrain graphics.[35]

The Way Ahead

Cyber operational graphics will allow the MAGTF commander to convey mission-essential information to his Marines who are unfamiliar with the technical details of cyberspace. Military tasks, missions, and operations share commonalities regardless of the domain in which they take place. Leveraging warfighter familiarity with a common language will enhance rapid understanding and decision making. These concepts only scratch the surface of an extremely large problem—the lack of joint cyber operational graphics. Giving the Marine Corps cyber/EFS community, the opportunity to take the lead, develop, and ultimately provide the MAGTF commander with a proven operational doctrine and the accompanying graphics that will enable him to understand, plan, fight, and win the cyber battle.

Notes

1. Maj Paul L. Stokes, "The Electronic Fire Support Coordinator," *Marine Corps Gazette* 95, No. 4 (2011). This article explains how a Marine communications officer can improve his ability to support combat operations by becoming "an operator/tactician" vice remaining in his comfort zone as "the technical guy."

2. Erick D. McCroskey and Charles A. Mock, "Operational Graphics for Cyberspace," *Joint Forces Quarterly* 85, No. 2 (2017).

3. MARFOR Cyber Warfare Group, Cyber Protection Teams, Communication Battalions, Marine Wing Communication Squadrons, Division & Marine Logistic Group Communication Companies, Radio Battalions, and Intelligence Battalions.

4. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: June 1997); and Headquarters Marine Corps, *MCDP 1-0, Marine Corps Operations*, (Washington, DC: September 2001); *MCDP 1-0, Marine Corps Operations*; and Headquarters Marine Corps, *MCDP 6, Command and Control*, (Washington, DC: October 1996).

5. Deputy Secretary of Defense Memorandum, *Definition of Cyberspace*, (Washington, DC: May 2008). Cyberspace is defined "as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and imbedded processors and controllers."

6. DOD Interface Standard, *Joint Military Symbology,* (Washington, DC: June 2014).

7. Institute for Defense Analyses, 4850 Mark Center Drive, Alexandria, VA. See *Operational Graphics for Cyberspace.*

8. Maj Paul L. Stokes and LtCol Barian A. Woodward, "The Cyber Base of Fire," *Marine Corps Gazette* 102, No. 4 (2018). This article explains how Marine Communicators/Cyber personnel can support combat operations via cyber maneuver.

9. Deputy Commandant Combat Development and Integration, *MAGTF Information Environment Operations (IE Ops) Concept of Employment (COE),* (Quantico: July 2017).

10. A *honeypot* is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, who are then blocked. This is similar to police sting operations colloquially known as "baiting," a suspect. Source https://en.wikipedia.org.

11. *Operational Graphics for Cyberspace.*

12. Joint Staff, *Joint Publication 3-12, Cyberspace Operations*, (Washington, DC: final revision draft, May 2017).

13. *Operational Graphics for Cyberspace.*

14. *MAGTF IE Ops COE*.

15. *Operational Graphics for Cyberspace.*

16. DOD, *DOD Instruction, Cybersecurity Activities Support to DoD Information Network Operations*, (Washington, DC: March 2016), incorporating Change 1, 25 July 2017. This instruction outlines DOD Cybersecurity policy. See also. *Operational Graphics for Cyberspace.*

17. Ibid.

18. Ibid.

19. Ibid.

20. Ibid.

21. Ibid.

22. Ibid.

23. Ibid.

24. Ibid.

25. Ibid.

26. Ibid.

27. Ibid.

28. Ibid.

29. DC CD&I, *MAGTF Defensive Cyberspace Operations Internal Defensive Measures (DCO-IDM) Company Concept of Employment (COE),* (Quantico, VA: July 2017).

30. *Operational Graphics for Cyberspace.*

31. Ibid.

32. Ibid.

33. Ibid.

34. *Phishing* is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (i.e., email, web link, or web post). Source: https://en.wikipedia.org/wiki/Phishing.

35. Ibid.

>*Author's Note: This article was adapted from "Operational Graphics for Cyberspace,"* Joint Force Quarterly*, 2nd Quarter, 2017.*