



Plane captain cleans canopy of EA-6B Prowler assigned to Electronic Attack Warfare Squadron 139 on flight deck of USS *Ronald Reagan*, Philippine Sea, June 19, 2006 (U.S. Navy/Kevin S. O'Brien)

Operational Graphics for Cyberspace

By Erick D. McCroskey and Charles A. Mock

The growth of any discipline depends on the ability to communicate and develop ideas, and this in turn relies on a language that is sufficiently detailed and flexible.

—SIMON SINGH, *FERMAT'S ENIGMA*

To promote interoperability at the information level within the area of joint military symbology, it is necessary to define a standard set of rules for symbol construction and generation to be implemented in C2 [command and control] systems.

—JOINT MILITARY SYMBOLOGY

A sergeant looks at an arrow marked in grease pencil on a laminated map and knows that a machine gun position lies ahead. The large projection screen showing a map with a blue rectangle encompassing an oval gives the joint task force commander assurance that a tank battalion defends key terrain. A picture is worth a thousand words.

Complex subjects—mathematics, chemistry, physics, even highway driving—have specialized sets of symbols that convey information and understanding more quickly than text alone can do. Symbols have been part of military tactics, operations, and strategy since armies became too large for personal observation on the battlefield. In joint military operations, it is crucial to have a set of common symbols familiar to all users. They are especially useful to establish a common understanding across a user population with widely varying knowledge, experience, and Service backgrounds. The Department of Defense (DOD) established the newest warfighting domain via doctrinal guidance 8 years ago, yet cyber warriors still lack a coherent set of symbols that allow them to convey the intricacies of cyber warfare to the joint warfighting community. The inability of cyber warriors to easily express operational concepts inhibits the identification of cyber key terrain, development of tactics and strategies, and execution of command and control.

DOD has a standard for joint military symbology, MIL-STD-2525D, *Joint Military Symbology*, which provides a set of cyberspace symbols in an appendix. 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 persona layers of cyberspace. The Institute for Defense Analyses provides analytical support for the director of the Operational Test and Evaluation

Cybersecurity Assessment Program, which evaluates cyberspace defensive operations during major exercises. To convey the operational context and importance of offensive and defensive cyber actions, we have developed a symbol set that is compliant with MIL-STD-2525, logically consistent, and capable of displaying the nuances of cyberwarfare to warfighters from all domains.

Why Graphics?

The primitive state of cyber operational graphics, and the resulting lack of effective communication between cyber and physical domain warriors, deemphasizes operational campaign design and the application of the principles of war in cyber operations. This increases the likelihood that physical domain warfighters will accept dangerous risks because they have little conception of what is really happening on their networks. In many ways, cyber units that are composed predominantly of governmental civilians and contractors resemble medieval mercenary artillery companies—formed to provide a necessary technical function, but not really considered soldiers. As artillery became more powerful, new tactics followed, and artillerymen became co-equal members of the total force. We are seeing the same evolution in cyber, as our technicians evolve into warfighters.

Cyber organizations do not lack for symbols and graphics—network diagrams are ubiquitous—but these symbols do not conform to joint warfighting doctrine. A firewall needs to be recognized as a fortification. A honeypot *is* an ambush site or a delaying obstacle in cyberspace. Scanning *is* reconnaissance, and networks *are* areas of responsibility. Cybersecurity service providers (CSPs) and enterprise operations centers are cyber defense 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. Militarizing cyber symbols will give the cyber warrior insight into the parallel and analogous activities performed in other domains.

Victory in a cyber-contested environment will come at an increased cost in time, material, and manpower. The U.S. Navy commands the seas and the Air Force has controlled the skies since World War II. Technological and tactical prowess give the Army and Marines a clear edge against all comers. Only in the cyberspace domain is the U.S. military hard pressed to defend itself, let alone the Nation. This is a vulnerability that adversaries will certainly seek to exploit. Yet many non-cyber military leaders have only a surface understanding of the implications. Militarization of cyber symbols will allow joint commanders to understand just what is happening in the cyber fight. The general might be unclear on what “Mimikatz” is or how it got through the firewall, but he will intuitively understand red arrows bypassing his fortifications and driving deep into his cyber key terrain. Commanders will soon 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 gradually be integrated into joint operations as doctrine evolves.

Doctrine is the ultimate beneficiary of cyber symbols that conform to a joint standard. Cyber warriors already know the basic tactics to secure the battlefield, but an inability to visualize the battle hampers creation of a nuanced flow of cyber combat. At the opposite end of the spectrum, Joint Publication (JP) 3-12, *Cyberspace Operations*, brought some order to cyber command and control, but the paucity of operational doctrine has left a gulf between the tactical and strategic. With proper symbols, concepts can be developed, presented, understood, and evolved by the joint community. Standards can be created—for example, how many defenders are necessary for 50,000 accounts? Basic military precepts such as tempo and attrition can be addressed in a cyber context. Operational requirements can be identified, and the systems and equipment needed to meet that need can be acquired. For cyberspace to truly become a warfighting domain, with all that entails, development of symbols that conform to joint standard is a necessary first step.

Colonel Erick D. McCroskey, USAF (Ret.), and Major Charles A. Mock, USMC (Ret.), are Research Staff Members in the Operational Evaluation Division at the Institute for Defense Analyses.

Figure 1. Cyberspace Terrain Description: Networks and Common Features

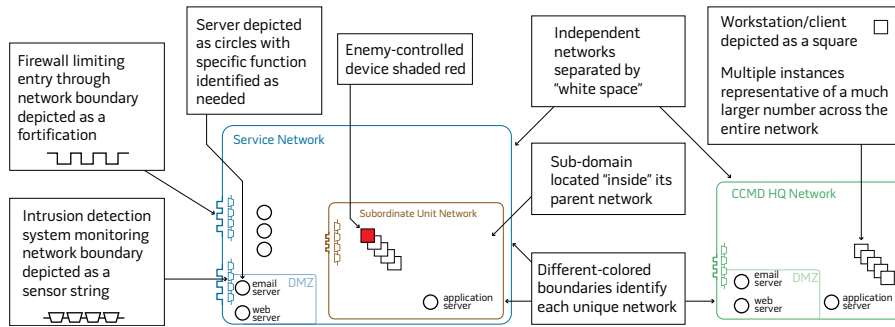
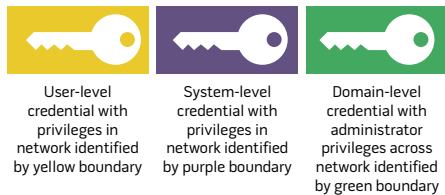


Figure 2. Notional Cyber Credential Icons



Terrain Graphics

Terrain is the fundamental medium for military action, in cyberspace as well as in the land, sea, and air domains. How terrain affects operations is different in all domains. JP 3-12 divides cyberspace into three layers: the physical, logical, and persona.

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 MIL-STD-2525D and are not addressed here.

The logical layer is where cyber terrain exists, and the primary cyberspace terrain feature is the network, a collection of devices that implement applications, services, and data stores. It is often governed by Internet protocol (IP) ports and addresses accessed through a router. Networks are the cyberspace equivalent to areas of operations in the physical domain, and their very existence is provisioned by assigned Domain Accreditation Authority, which issues policy guidance and exercises some degree of command and control over subordinate units within the mission category of

DOD information network operations (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 and local cyber defenders (as prescribed in DOD Instruction 8530.01), it is analogous to the most common command and control area designation: the operational area (OA).

We choose to depict individual networks by the devices they comprise with a unique boundary line that represents the extent of the IP address space within it (see figure 1). For clarity, we typically depict only sufficient numbers of devices necessary to describe the planned or observed cyberspace operations, or to convey understanding of the nature of the terrain. For instance, if only one device out of hundreds on the network is attacked, we may choose to show that device alongside a half-dozen others, often with a note that the small number of devices depicted is representative of many more. We also choose to use unique color-coded boundaries for each network to enable quick understanding of the terrain because relatively few unique networks are typically required to depict a cyberspace battle and because alphanumeric designations 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.

Cyberspace terrain is unique in that 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. Cyberspace terrain is also changeable on short timescales. If you do not like how the enemy is using your terrain, you 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 has little meaning in operational graphics depictions. However, the relationships between networks, such as where one is a sub-domain of another, are important, so we depict subdomains as existing completely within their parent networks.

Devices in cyberspace generally function simultaneously as terrain features on which forces maneuver and as installations (which provide necessary supply, transportation, command and control, defensive, surveillance, or other warfighting functions); thus, they have no clear analogies in the physical domain. We adopt common network diagram symbols in simplified form depicting an individual workstation or client as a square and a server as a circle. However, we depict two specialized devices (and the functions they perform) that are nearly always present in cyber battles with unique symbols: the firewall is represented as a fortification, and the intrusion detection equipment and services are represented as a string of sensors.

Similar to its physical counterpart, a cyberspace 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 stores—within the OA without the defenders being aware of the compromise. This situation is analogous to insurgency operations, in which 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

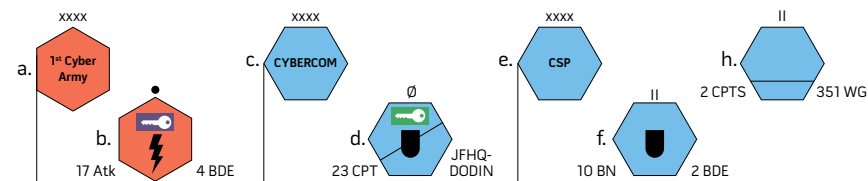
defenders do not realize that they ought to sever the connections between the OA and the rest of the network—a prime mission for special forces. Red shading represents devices that have fallen under enemy control in some way. In some instances, red shading may be used to represent enemy control over an entire network.

Persona and Credential Graphics

The persona layer is the means by which personnel and units operate in cyberspace. JP 3-12 rightly asserts that the cyber persona layer requires a higher level of abstraction, but the publication introduces confusion when it states that the persona layer consists of people actually on the network. People do not exist in cyberspace, of course. Accounts and their associated credentials (usernames, passwords, Common Access Cards, personal identification numbers, and so forth) are the primary cyber entities that operators use to execute administrative actions, domain control, user activity, printer access, or any number of function-related activities. While we tend to think of accounts as being people, it is more logical to think of accounts in terms of cyber equipment used by operators existing in the physical domains. For example, in the air domain, a pilot (the operator) uses an F-22 (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-22 operator is physically paired with his equipment in the air domain itself, whereas the cyber operator resides in the physical domain (where the physical layer of cyberspace exits) and conducts his mission in the cyberspace domain via the logical and persona layers, “looking in from the outside.” Cyber units thus have a foot in two domains: the living operators and physical layer hardware in one domain, and the mixed types of accounts, credentials cyber actions, and missions in another.

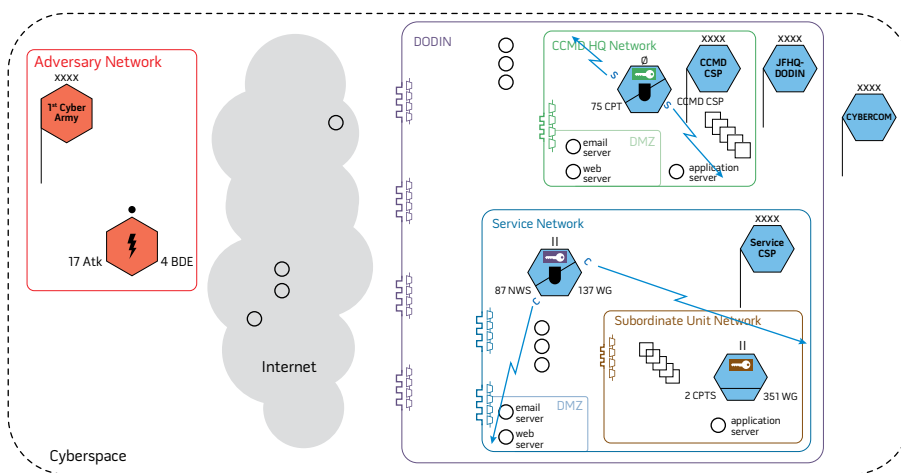
Credentials are the keys to the cyber equipment and associated accesses and

Figure 3. Notional Cyber Unit Icons



Key: a. Adversary headquarters (HQ); b. Adversary squad-level offensive cyberspace operations unit with captured system admin credentials; c. U.S. Cyber Command HQ; d. Friendly Defensive Cyberspace Operations (DCO) unit with reconnaissance capabilities that has been granted domain administration credentials/authorities; e. Friendly cybersecurity service provider HQ; f. Friendly DCO unit; h. Friendly DODIN ops cyber unit

Figure 4. Notional Cyberspace Terrain Showing Boundaries, Units, and Defensive Tasks



privileges. Adversary control of a user-level account is damaging because it allows the enemy to traverse the OA in the guise of a friendly operator. An adversary who gains credentialed access to a domain administration account is able to use the privileges associated with this account to control all the key terrain—accounts, servers, data, and applications—in that OA. Different key symbols reinforce this 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 (see figure 2).

Unit Graphics

MIL-STD-2525D prescribes the use of specific frames for icon-based symbols to depict the identities of units operating in the land, sea, air, space, and subsurface physical domains. It does



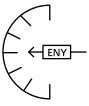

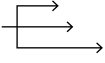



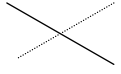
not prescribe a unique frame to identify units when depicting operations solely in cyberspace (that is, the logical and persona layers). We adopt a regular hexagonal frame to depict units in cyberspace. We use standard shading conventions for friendly, neutral, hostile, civilian, and unknown standard identities and rotate the hexagons by 30° to depict hostile units (figure 3).

Icons, defined in MIL-STD-2525D as “the innermost part(s) of a symbol which provides an abstract pictorial or alphanumeric representation of units, equipment, installations, activities, or operations,” must necessarily represent the unique nature of cyberspace units. Cyberspace personnel receive training for particular missions using specialized software, hardware, and network “equipment.” However, the generally applicable nature of the equipment, techniques, and

Table. Adaptation of Tactical Task Graphics to Cyberspace

Tactical Task	Operational Graphic	Doctrinal Description*	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 the 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 adversary 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 practitioner (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 rely upon fires and combat support assets of the main body.	Domain-wide detection and hunt-type activities by a cyber protection Team 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 reposturing 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 Soldiers or units from areas under enemy control by stealth, deception, surprise, or clandestine means.
Occupy		Remove Soldiers 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, or clandestine means.
Retain		Remove Soldiers 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, or clandestine means.
Secure		Remove Soldiers 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, or clandestine means.
Seize		Remove Soldiers 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, or clandestine means.
Support by fire		Remove Soldiers 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, or clandestine means.

Table. Adaptation of Tactical Task Graphics to Cyberspace

Tactical Task	Operational Graphic	Doctrinal Description*	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 force 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 to 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) services, 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 materiel 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).

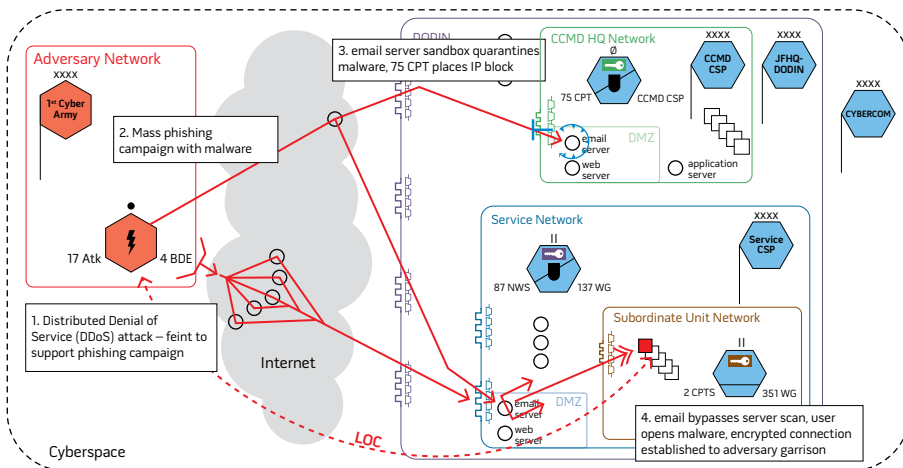
* As described and depicted in various DOD sources, including MIL-STD-2525D, *Joint Military Symbolology*, June 10, 2014; Field Manual (FM) 1-02/Marine Corps Reference Publication 5-12A, *Operational Terms and Graphics*, February 2, 2010 (incorporating Change 1); FM 3-90-1, *Offense and Defense*, vol. 1, March 2013; FM 3-90-2, *Reconnaissance, Security and Tactical Enabling Tasks*, vol. 2, March 2013.

core technical skills allows cyber personnel and units to perform diverse functions (for example, reconnaissance, identification friend or foe, command and control, creating or modifying terrain features,

engaging targets, occupying terrain) that are often required to execute typical missions, whereas units in the physical domain tend to have a more specialized set of functions based on their training

and equipment. Although cyber units may be equipped with specific “platforms” and trained for unique missions at the lowest tactical levels, in general the diversity of the functions that cyber forces

Figure 5. Sequential Actions in the Initial Adversary Assault: A Feint, Blocked Phishing Attack, Successful Bypass of Defenses That Gains Control of Friendly Terrain



are capable of prohibits unique categorization by unit type based on specific equipment or mission as is typical in the physical domains (for example, infantry versus mechanized infantry versus armor battalions, F-22 versus E-3 versus KC-135 squadrons). Instead, we use symbols that identify cyber units based on which of the three general mission categories from JP 3-12 they typically perform: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DODIN ops. A lightning bolt identifies OCO units, a shield icon identifies DCO units, and existing support unit iconography identifies DODIN ops units.

Cyber warriors often regard detection as the most critical of their tasks, and individual cyber units are often assigned “detect” as a priority mission and are specially equipped and trained to execute it. Cyber 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.

Cyber units are identified by the echelon command level to which they belong, just as units in the physical domain are, but the reader 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” (for example, an infantry battalion may have 500 persons assigned and fight on a front of perhaps a half-mile in extent, while a fighter squadron may have 150 persons and 24 aircraft assigned and fight within a 500-mile radius of its base). The variation between cyber and physical units within the same echelon, however, tends to be even greater. For example, a cyber battalion or squadron primarily responsible for *global* detection and response efforts for an entire service network might have 300 persons assigned. Additionally, there tend to be substantially fewer units at any given echelon within the total cyber force structure. We choose to adopt the existing echelon representation (used primarily in representing land force units) and apply it using the official designations of cyberspace units, with cyber protection teams representative of the lower echelons of friendly cyber forces typically portrayed, and U.S. Cyber Command as the top echelon.

Cyberspace commanders would benefit from decision graphics showing unit combat effectiveness, specific platform equipment and capabilities, and task organization composition, similar to those used tactically and operationally in the physical domains, but we defer this level of detail until cyberspace doctrine

matures to the point that these can be useful in the planning and execution of battles and campaigns.

Mission Graphics

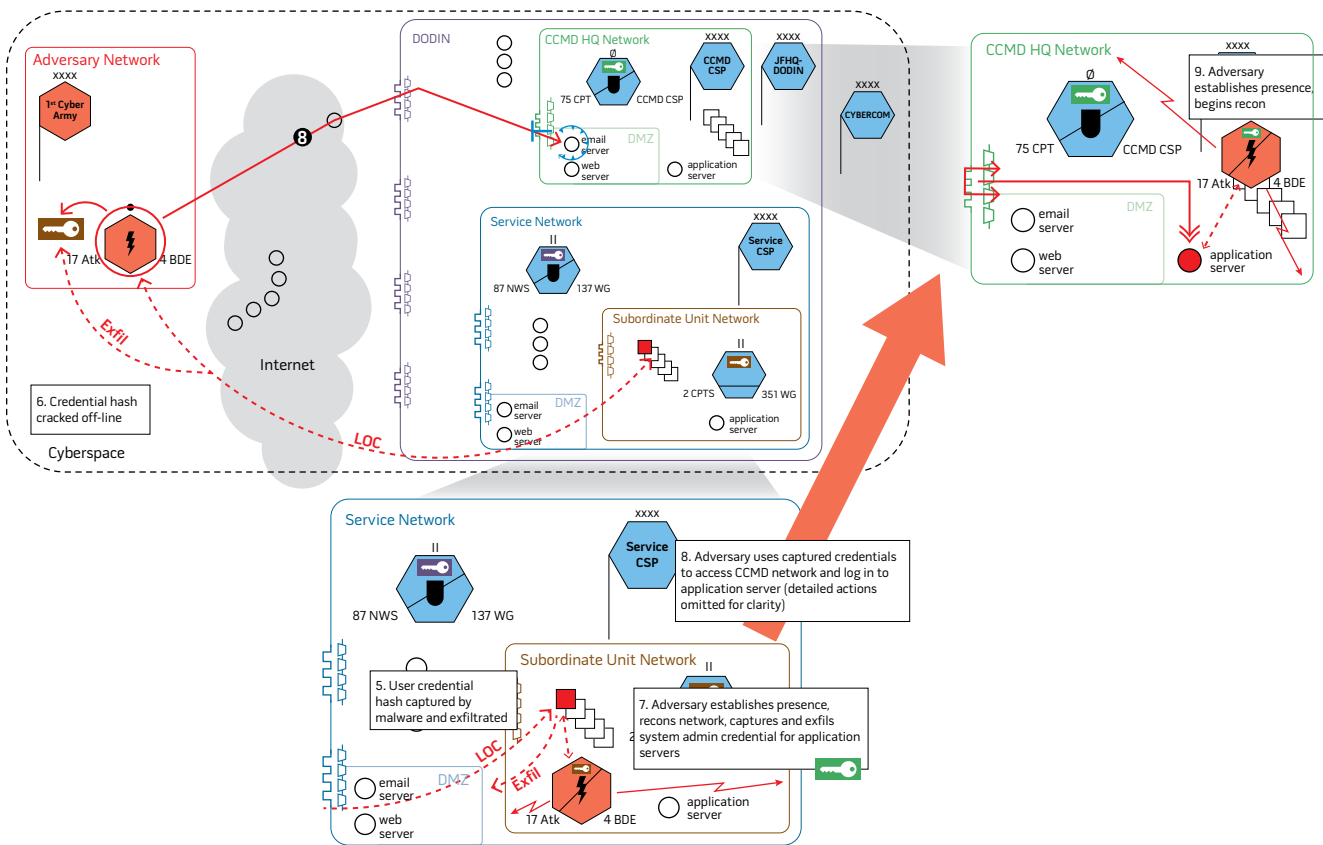
Although some graphic control measures used in the land domain (such as phase lines, assembly areas, fire support coordination measures, and check-points) may not be useful in describing operations in cyberspace, others can be readily adapted for the purposes of planning and maintaining situational awareness. 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 of communication 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 the table.

Other tactical tasks potentially useful for describing cyberspace actions were omitted from the table for the sake of brevity or because no associated operational graphic exists: control, counter-reconnaissance (area security, local security), disengage, follow and assume, follow and support, defeat, and suppress.

Putting It All Together

These basic building blocks allow portrayal of cyber battles in a straightforward manner and present the action to the joint warfighter in a familiar format. The symbol set is still small—units, terrain, command and control, attack vectors—but capable of providing insights the commander needs for a rudimentary situational awareness of the operational area. Combatant command J6s already understand why firewalls and sensors are ineffective once an adversary 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 joint force commander with

Figure 6. Subsequent Adversary Actions on Friendly Terrain: Seizing of Credentials, Reconnaissance, and Lateral Movement Within and Between Networks



an understanding—an enormous red flag signaling risk to his mission—that has been missing from the cyber portion of joint warfighting.

Figures 4, 5, and 6 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 culminating in the penetration of defenses and the attacker occupying defended territory and postured to conduct follow-on operations. The astute reader will notice the similarities to historical depictions of Civil War battlefields, which motivated the development of these graphics to clearly depict complex, sequential actions over extended durations.

Conclusion

Cyberspace operational graphics will allow cyber planners and operators to convey mission-relevant information to

warfighters 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, and leveraging warfighter familiarity with the common language that has evolved to describe them will enhance rapid understanding and decisionmaking.

The concepts presented here only scratch the surface of an extremely large problem. To date, there is little official recognition that the cyber community should even conform to joint symbology standards. Cyber symbols merit only 3 of the 885 pages of MIL-STD-2525D. If DOD intends to treat cyberspace as a warfighting domain, then standards must reflect that guidance. However, that is just the beginning.

Using operational graphics to describe cyberspace actions should lead to the identification of parallels and analogies in the physical domains that

could potentially be implemented in cyberspace operational doctrine. For instance, the doctrinal concepts of culmination and attrition that are critical to operational campaign design and execution in the physical domains may finally be examined fully for application in the cyber domain. Ultimately, the joint commander will have at his disposal a coherent body of operational doctrine and the accompanying graphics that will enable him to understand, plan, and fight the cyber battle. JFQ

The authors would like to extend their appreciation to Robert Soule and Dr. Shawn Whetstone from the Institute for Defense Analyses for their continued support and encouragement in developing these ideas, and to Dr. J. Michael Gilmore, Dr. Kenneth M. Crosswait, and Dan Burgess from Director, Operational Test and Evaluation, for recognizing the utility of cyberspace operational graphics, for their insightful feedback, and for their continuing challenge to us to improve the concepts.