Operational Graphics for Cyberspace

Erick D. McCroskey and Charles A. Mock

The Challenge: Specialized sets of symbols that convey information and understanding faster than text alone have been part of military tactics, strategy, and the operational art since armies became too large for personal observation on the battlefield. The Department of Defense (DoD) established cyberspace as the newest warfighting domain via doctrinal guidance in 2011, 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 identification of cyber key terrain, the development of tactics and strategies, and the execution of command and control.

Cyber organizations do not lack for symbols and graphics—network diagrams are ubiquitous—but these symbols do not conform to joint warfighting doctrine.

Introduction

A sergeant looks at an arrow marked in grease pencil on a laminated map and knows that a machinegun 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.

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.

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 (CSSP) 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. The Internet is no longer just the Internet; it's the battlefield.

Militarizing cyber symbols will give the cyber warrior insight into the parallel and analogous activities performed in other domains and 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 air-land-sea battle, must and will gradually be integrated into joint operations as doctrine evolves.

Doctrine will ultimately benefit from cyber symbols that conform to a joint standard. Cyber warriors already know the basic tactics for securing 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 3-12 (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 the strategic. With proper symbols, concepts can be developed, presented, understood, and evolved by the joint community. Standards can be created, e.g., 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. To meet this need, IDA researchers 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.

Terrain Graphics

JP 3-12 divides cyberspace into three layers: the physical, the logical, and the 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, *Joint Military Symbology*, 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. Networks are the cyberspace equivalent to areas of operations in the physical domain. 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, it is analogous to the most common command and control area designation: the operational area (OA).

We depict individual networks with a unique color-coded boundary line that represents the extent of the IP address space within it (see Figure 1).

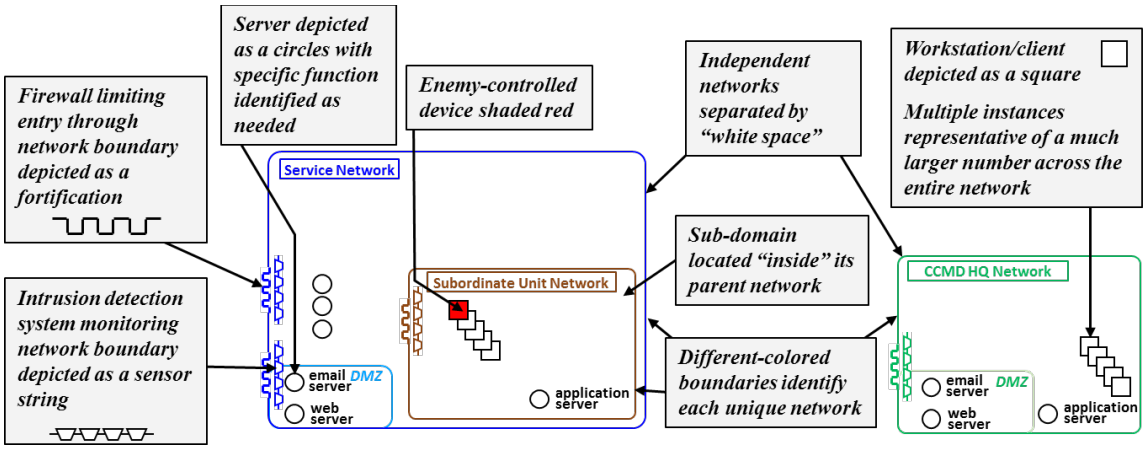


Figure 1. Cyberspace terrain description – networks and common features

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 half a dozen others, often with a note that the small number of devices depicted are representative of many more.

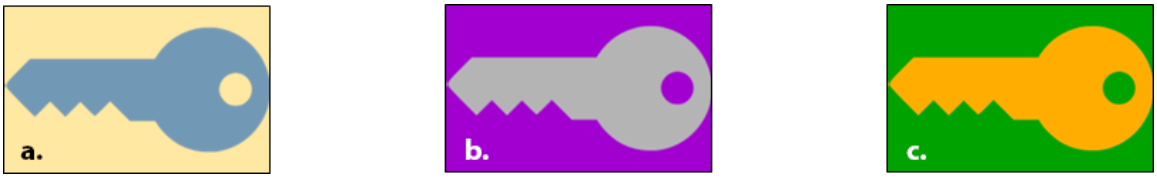
Because of the nature of cyberspace, the distance between and the relative positioning of unique independent networks have little meaning in operational graphics depictions. However, the relationships between networks, such as one being a subdomain of another, *is* important, so we depict subdomains as existing completely within their parent networks.

Devices in cyberspace generally function simultaneously as terrain features upon 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 fortification, and the intrusion detection equipment and services are represented as a string of sensors.

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 introduces confusion when it states that the persona layer consists of the people actually on the network. People do not exist in cyberspace, of course. Accounts and



a. user-level credential with privileges in network identified by yellow boundary

b. system-level credential with privileges in network identified by purple boundary

c. domain-level credential with administrator privileges across network identified by green boundary

Figure 2. Notional cyber credential icons

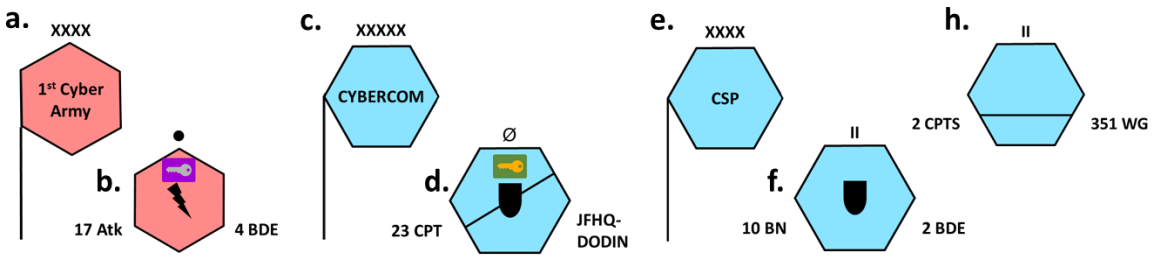
their associated credentials (e.g., usernames, passwords, Common Access Card PIN) are the primary cyber entities that operators use to execute administrative actions, domain control, user activity, printer access, or any number of function-related activities—a network user account is a piece of cyber equipment that allows the operator to conduct email, use an Microsoft Office application, or communicate with other accounts. Similarly, in the air domain, a pilot (the operator) uses an F-22 (a piece of equipment) to conduct a variety of air superiority missions.

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. 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 privileges. An adversary who gains credentialed access to a domain administration account is able to use the privileges associated with this account to control all of the key terrain—accounts, servers, data, and applications—in that OA. Different key symbols reinforce this point: blue for user-level, silver for system-level, and gold 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. We adopt a regular hexagon frame to depict units in cyberspace (i.e., the logical and persona layers). We use standard colors for friendly and hostile entities and rotate the hexagons by 30 degrees to depict hostile units (Figure 3).



a. adversary HQ

b. adversary squad-level OCO unit with captured system admin credentials

c. U.S. Cyber Command HQ

d. friendly DCO unit with reconnaissance capabilities that has been granted domain admin credentials/authorities

e. friendly Cybersecurity Service Provider HQ

f. friendly DCO unit

h. friendly DODIN Ops cyber unit

Figure 3. Notional cyber unit icons

An icon, the innermost part of a symbol that provides an abstract pictorial or alphanumeric representation of units, equipment, installations, activities, or operations, must necessarily represent the unique nature of cyberspace units. Although cyber units may be equipped with specific "platforms" and trained for very specialized, unique missions at the lowest tactical levels, in general the diversity of the functions that cyber forces are capable of prohibits unique categorization by unit type based on specific equipment or mission as is typical in the physical domains (e.g., 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 DoD Information Network (DoDIN) Operations. A lightning bolt identifies OCO units, a shield icon identifies DCO units, and existing support unit iconography identifies DoDIN Operations units. 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.

We chose 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.

Mission Graphics

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 Table 1. The Doctrinal Description is as described and depicted in various DoD sources, including MIL-STD-2525D.

Other tactical tasks potentially useful for describing cyberspace actions were omitted from Table 1 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.

Table 1. Adaptation of Tactical Task Graphics to Cyberspace

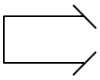
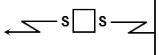
Tactical Task	Operational Graphic	Doctrinal Description	Potential Use in Describing Cyberspace Operations
ACTIONS BY FRIENDLY FORCE			
Attack by fire		The use of direct fires, supported by indirect fires, to engage an enemy force without closing with the enemy to destroy, suppress, fix, or deceive that 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.	Non-credential-based access (e.g., 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 CSSP.
Counter-reconnaissance (Screen)		Provide early warning to the protected force.	Detection activities on a boundary or domain.

Table 1. Adaptation of Tactical Task Graphics to Cyberspace (continued)

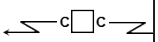
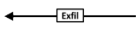
Counter-reconnaissance (Guard)		Protect the main body by fighting to gain time while also observing and reporting information and preventing enemy ground observation of and direct fire against the main body. Units conducting a guard mission cannot operate independently because they rely upon fires and combat support assets of the main body.	Domain-wide detection and hunt-type activities by a Cyber Protection Team (CPT) or local defensive unit, augmenting the capabilities of a CSSP.
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 CSSP.
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.	Movement of data from its original location to a location under enemy control, typically by means of stealth, deception, 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 of the area occur without enemy opposition.	Deployment of a CPT to a domain in advance of suspected adversary 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 adversary 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 adversary 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 cyberspace, 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 maneuvering force.	Overt actions where an origination (or interim relay) point can be determined, such as Distributed Denial of Service attacks and, broad intrusive scans, and where these actions are designed to set the conditions for success for the primary attack actions.

Table 1. Adaptation of Tactical Task Graphics to Cyberspace (continued)

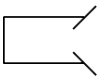
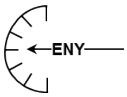
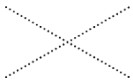
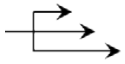
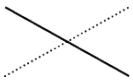
EFFECTS ON ENEMY FORCE			
Block		Deny the enemy access to an area or prevent the enemy's advance in a direction or along an avenue of approach. Also an obstacle effect that integrates fire planning and obstacle efforts to stop an attacker along a specific avenue of approach or prevent the attacking force from passing through an engagement area.	Use or modification of blacklists, whitelists, access control lists, routing policies, credentials (username-password pairs or machine-issued), filters on firewalls, DNS 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 BIOS 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.

Table 1. Adaptation of Tactical Task Graphics to Cyberspace (continued)

EFFECTS ON ENEMY FORCE			
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 (e.g., reboot a domain controller or data server following an induced system crash); to expend much greater effort than planned to obtain an objective (e.g., consuming attacker resources using a realistic honeynet); or to refrain from using capabilities for fear of detection (e.g., 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 (e.g., interrupt the sensor feeds from a target domain to the responsible cyber defense unit).

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 his OA. For example, 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 an enormous red flag that signals risk to the mission, which 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.

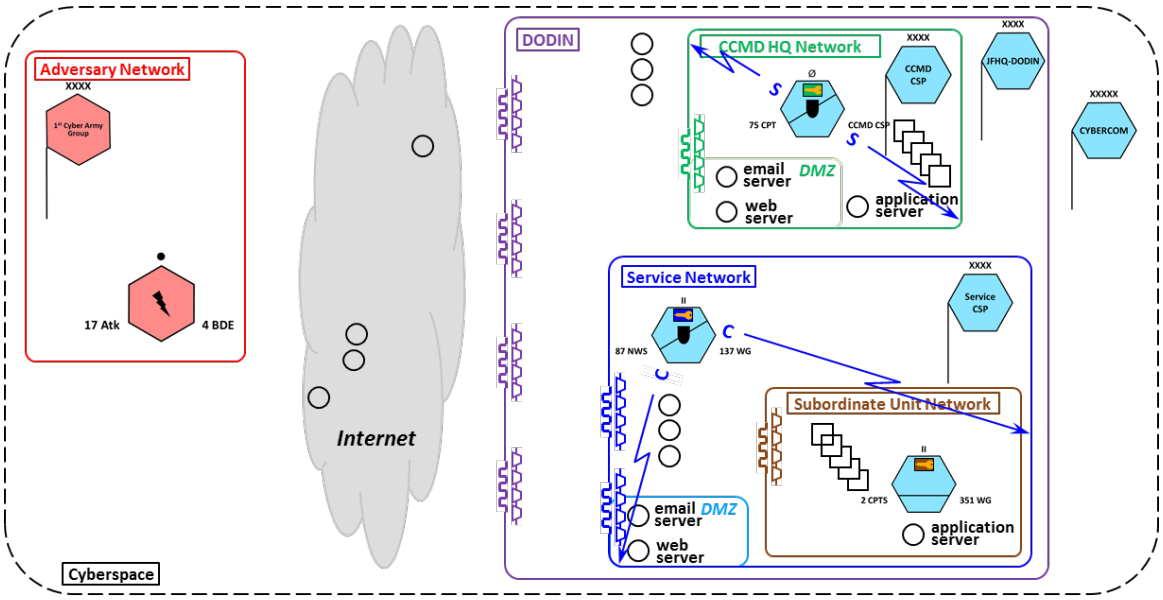


Figure 4. Notional cyberspace terrain showing boundaries, units, and defensive tasks

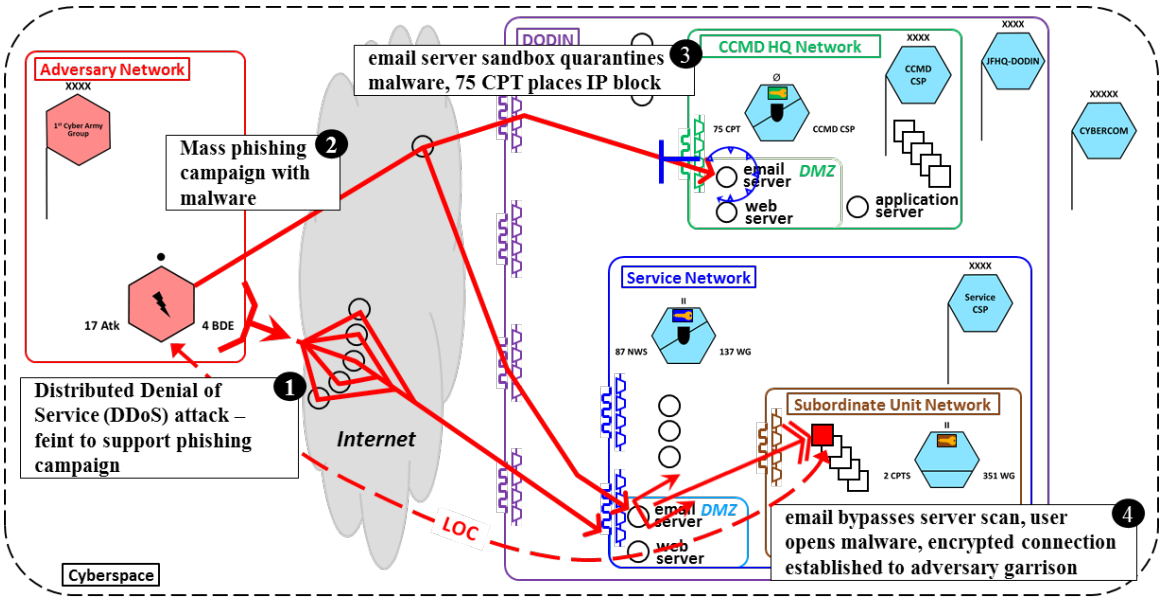


Figure 5. Sequential actions in the intial adversary assault: a feint, a blocked phishing attack, and a successful bypass of the defenses that gains control of friendly terrain

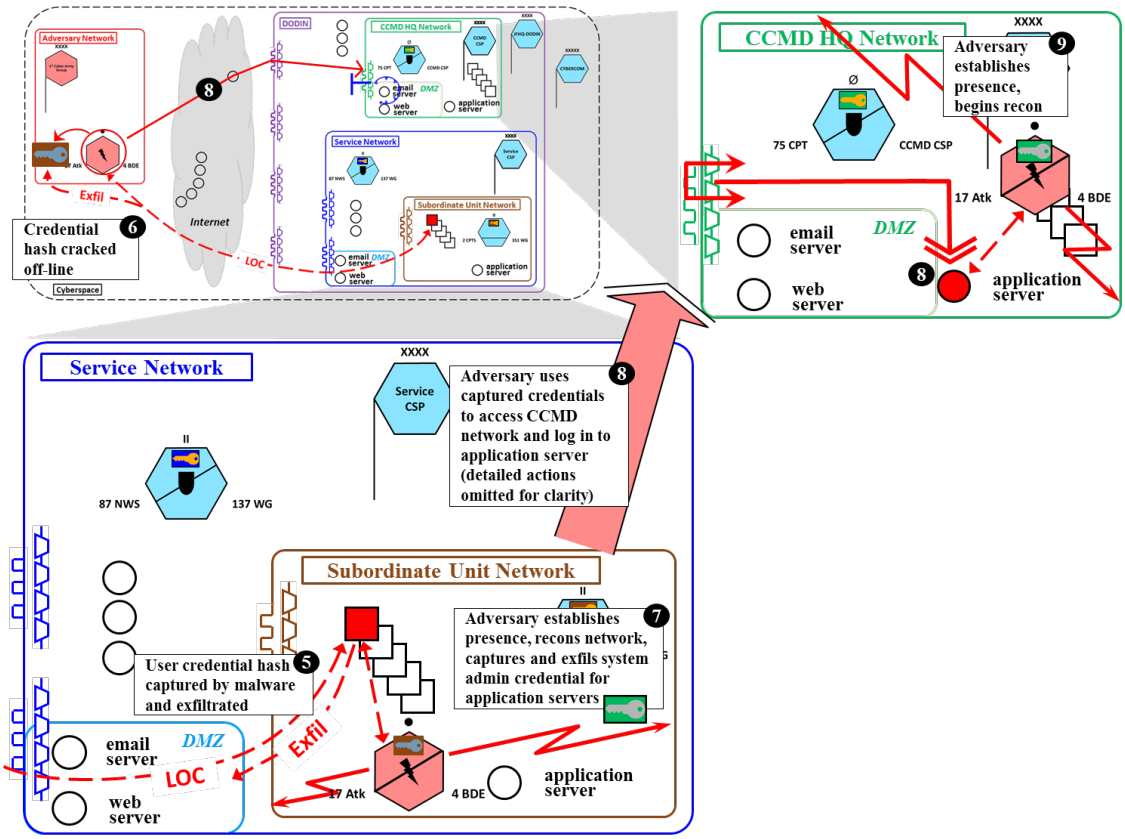


Figure 6. Subsequent adversary actions on friendly terrain: seizing of credentials, reconnaissance, and lateral movement within and between networks

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 decision-making.

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 enable him to understand, plan, and fight the cyber battle.

IDA hosted the first-ever DoD Cyber Symbology Workshop in February 2019, and the symbol set is in the process of being refined and formally incorporated into MIL-STD-2525 by DoD.

Reference

MIL-STD-2525D, Joint Military Symbology, 10 June 2014; FM-102/MCRP 5-12A, Operational Terms and Graphics, 2 February 2010 (incorporating Change 1); FM 3-90-1, Offense and Defense, Volume 1, March 2013; FM 3-90-2, Reconnaissance, Security and Tactical Enabling Tasks, Volume 2, March 2013.

Mr. Erick D. McCroskey is an Adjunct Research Staff Member in IDA's Operational Evaluation Division. He holds a Master of Science in applied engineering (physics) from the University of California, Davis, and a Master of Arts in military arts and sciences from the School of Advanced Military Studies, Fort Leavenworth.

Mr. Charles A. Mock is a Research Staff Member in IDA's Operational Evaluation Division. He holds a Master of Science in computer science from the Naval Postgraduate School.