بسمه تعالی

جمهوری اسلامی ایران

فرماندهی کل قوا

ستاد کل نیروهای مسلح

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

دفترچه زبان انگلیسی

ویژه مصاحبه دوره دکتری (Ph.D)

رشته مدیریت راهبردی فضای سایبر

سال تحصیلی ۱۴۰۲-۱۴۰۱

Layers: Cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona (see Figure 1). Each layer represents a different focus from which Cyberspace Operations (CO) may be planned, conducted, and assessed.

(1) The **physical network layer** consists of the information technology (IT) devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components. The physical network components include the hardware and infrastructure (e.g., computing devices, storage devices, network devices, and wired and wireless links). Every physical component of cyberspace is owned by a public or private entity, which can control or restrict access to their components. These unique characteristics of the OE must be taken into consideration during all phases of planning.

(2) The **logical network layer** consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node, but to their ability to be addressed logically and exchange or process data). Individual links and nodes are represented in the logical layer but so are various distributed elements of cyberspace, including data, applications, and network processes not tied to a single node. An example is the Joint Knowledge Online Website, which exists on multiple servers in multiple locations in the physical domains but is represented as a single URL [uniform resource locator] on the World Wide Web.

(3) The **cyber-persona layer** is a view of cyberspace created by abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another. Cyber-personas may relate directly to an actual person or entity. One individual may create and maintain multiple cyber-personas through use of multiple identifiers in cyberspace, such as separate work and personal email addresses, and different identities on different Web forums, chat rooms, and social networking sites, which may

vary in the degree to which they are factually accurate. Conversely, a single cyber-persona can have multiple users, such as multiple hackers using the same malicious software (malware) control alias, multiple extremists using a single bank account, or all members of the same organization using the same e-mail address. The use of cyber-personas can make attributing responsibility for actions in cyberspace difficult.

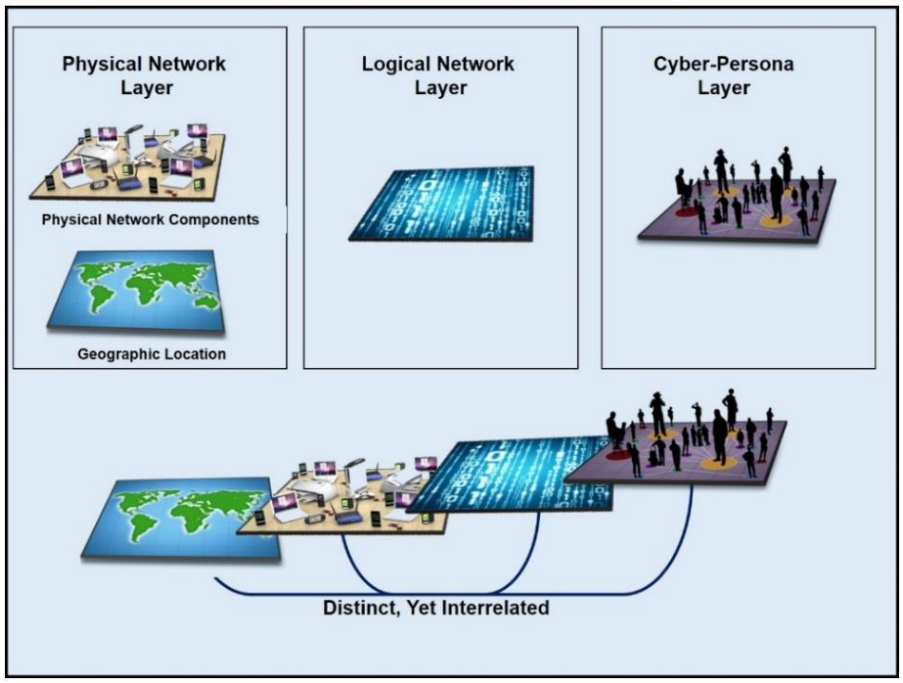

Figure 1: The Three Layers of Cyberspace

Cyberspace Location and Ownership. Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations.

a. **Blue Cyberspace** denotes areas in cyberspace protected by the United States, its mission partners, and other areas DOD may be ordered to protect. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare, on order, and when requested by other authorities, to defend or secure other USG or other cyberspace, as well as cyberspace related to critical infrastructure and key resources (CI/KR) of the United States and Partner Nations (PNs).

b. **Red Cyberspace** refers to those portions of cyberspace owned or controlled by an adversary or enemy. In this case, "controlled" means more than simply "having a presence on," since threats may have clandestine access to elements of global cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, controlled means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others.

c. **Gray Cyberspace**. All cyberspace that does not meet the description of either "blue" or "red" is referred to as "gray" cyberspace.

Cyber Threats. Cyberspace presents the commander with many threats ranging from nation-states to individual actors.

a. **Nation State Threat**. This threat is potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to other actors. Some nations may employ cyberspace capabilities to attack or conduct espionage against the United States. Nation-state threats involve traditional adversaries; enemies; and potentially, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.

b. **Non-State Threats**. Non-state threats are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs), and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct direct terrorist actions within cyberspace. Criminal organizations may be national or transnational in nature and steal information for their own use, including selling it to raise capital and target financial institutions for fraud and theft of funds. They may also be used as surrogates by nation-states or non-state threats to conduct attacks or espionage through cyberspace.

c. **Individual Actors or Small Group Threat**. Even individuals or small groups of people can attack or exploit U.S. cyberspace, enabled by affordable and readily available techniques and malware. Their intentions are as varied as the number of groups and individuals. These threats exploit vulnerabilities to gain access to discover additional vulnerabilities or sensitive data or maneuver to achieve other objectives. Ethical hackers may share the vulnerability information with the network

owners, but, more frequently, these accesses are used for malicious intent. Some threats are politically motivated and use cyberspace to spread their message. The activities of these small-scale threats can be co-opted by more sophisticated threats, such as criminal organizations or nation-states, often without their knowledge, to execute operations against targets while concealing the identity of the threat/sponsor and also creating plausible deniability.

d. **Accidents or Natural Hazards**. The physical infrastructure of cyberspace is routinely disrupted by operator errors, industrial accidents, and natural disasters. These unpredictable events can have greater impact on joint operations than the actions of enemies. Recovery from accidents and hazardous incidents can be complicated by the requirement for significant coordination external to DOD and/or the temporary reliance on back-up systems with which operators may not be proficient.

Challenges: In addition to the threats mentioned above, the commander must address significant cyberspace challenges when defining the problem and producing an operationalapproach.

a. **Anonymity and Difficulties with Attribution**. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable. This effort requires significant analysis and, often, collaboration with non-cyberspace agencies or organizations. The ability to hide the sponsor and/or the threat behind a particular malicious effect in cyberspace makes it difficult to determine how, when, and where to respond. The design of the Internet lends itself to anonymity and, combined with applications intended to hide the identity of users, attribution will continue to be a challenge for the foreseeable future.

b. **Geography Challenges**. In cyberspace, there is no stateless maneuver space. Therefore, when U.S. military forces maneuver in foreign cyberspace, mission and policy requirements may require they maneuver clandestinely without the knowledge of the state where the infrastructure is located. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external

operations in red and gray cyberspace, as well as internal protection effects in blue cyberspace.

c. **Technology Challenges**. Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. Cyberspace capabilities without hardware components can be replicated for little or no cost. This means that once discovered, these capabilities will be widely available to adversaries, in some cases before security measures in the DODIN can be updated to account for the new threat. In addition, since similar technologies around the world share similar vulnerabilities, a single adversary may be able to exploit multiple targets at once using the same malware or exploitation tactic. Malware can be modified (or be designed to automatically modify itself), complicating efforts to detect and eradicate it.

Assessment of Cyberspace Threats: In April 2021, the Director of National Intelligence (DNI) stated "Cyber threats from nation states and their surrogates will remain acute. Foreign states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure. Although an increasing number of countries and nonstate actors have these capabilities, we remain most concerned about Russia, China, Iran, and North Korea. Many skilled foreign cybercriminals targeting the United States maintain mutually beneficial relationships with these and other countries that offer them safe haven or benefit from their activity."

a. **Transnational Threats**. States' increasing use of cyber operations as a tool of national power, including increasing use by militaries around the world, raises the prospect of more destructive and disruptive cyber activity. As states attempt more aggressive cyber operations, they are more likely to affect civilian populations and to embolden other states that seek similar outcomes.

> (1) Authoritarian and illiberal regimes around the world will increasingly exploit digital tools to surveil their citizens, control free expression, and censor and manipulate information to maintain control over their populations. Such regimes are increasingly conducting cyber intrusions that affect citizens beyond their borders – such as hacking journalists and religious minorities or attacking tools that allow free speech online – as part of their broader efforts to surveil and influence foreign populations. Democracies will continue to debate how to protect privacy and civil liberties as they confront domestic security threats and contend with the perception that free speech may be

constrained by major technology companies. Authoritarian and illiberal regimes, meanwhile, probably will point to democracies' embrace of these tools to justify their own repressive programs at home and malign influence abroad.

(2) During the last decade, state sponsored hackers have compromised software and IT service supply chains, helping them conduct operations – espionage, sabotage, and potentially prepositioning for warfighting.

b. **China**. The DNI assessed that China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat. China's cyber pursuits and proliferation of related technologies increase the threats of cyber-attacks against the US homeland, suppression of US web content that Beijing views as threatening to its internal ideological control, and the expansion of technology-driven authoritarianism around the world.

(1) China can launch cyber-attacks that, at a minimum, can cause localized, temporary disruptions to critical infrastructure within the United States.

(2) China leads the world in applying surveillance systems and censorship to monitor its population and repress dissent, particularly among ethnic minorities, such as the Uyghurs. Beijing conducts cyber intrusions that affect US and non-US citizens beyond its borders – such as hacking journalists, stealing personal information, or attacking tools that allow free speech online – as part of its efforts to surveil perceived threats to the Chinese Communist Party (CCP) power and tailor influence efforts. Beijing is also using its assistance to global efforts to combat COVID-19 to export its surveillance tools and technologies.

(3) China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations.

c. **Russia**. The DNI assessed that Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

(1) Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves – and in

some cases can demonstrate – its ability to damage infrastructure during a crisis.

(2) A Russian software supply chain operation in 2020, described in the cyber section of this report, demonstrates Moscow's capability and intent to target and potentially disrupt public and private organizations in the United States.

(3) Russia is also using cyber operations to defend against what it sees as threats to the stability of the Russian Government. In 2019, Russia attempted to hack journalists and organizations that were investigating Russian Government activity and in at least one instance leaked their information.

(4) Russia almost certainly considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.

(5) A Russian software supply chain operation against a US-based IT firm exposed approximately 18,000 customers worldwide, including enterprise networks across US Federal, state, and local governments; critical infrastructure entities; and other private sector organizations. The actors proceeded with follow-on activities to compromise the systems of some customers, including some US Government agencies.

d. **Iran**. The DNI stated that Iran's expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US and allied networks and data. Iran has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities. Iran is increasingly active in using cyberspace to enable influence operations … and we expect Tehran to focus on online covert influence, such as spreading disinformation about fake threats or compromised election infrastructure and recirculating anti-US content.

(1) Iran was responsible for multiple cyber-attacks between April and July 2020 against Israeli water facilities that caused unspecified short-term effects, according to press reporting.

(2) Iran attempted to influence dynamics around the 2020 US presidential election by sending threatening messages to US voters, and Iranian cyber actors in December 2020 disseminated information about US election officials to try to undermine confidence in the US election.

e. **North Korea**. The DNI assessed that North Korea's cyber program poses a growing espionage, theft, and attack threat.

(1) Pyongyang probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States, judging from its operations during the past decade, and it may be able to conduct operations that compromise software supply chains.

(2) North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs.

f. **Terrorists**. The DNI testified that "terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims. Terrorist groups could cause some disruptive effects – defacing websites or executing denial-of-service attacks against poorly protected networks – with little to no warning."

g. **Criminals**. The DNI stated that "foreign cyber criminals will continue to conduct for profit, cyber-enabled theft and extortion against US networks. We anticipate that financially motivated cyber criminals very likely will expand their targets in the United States in the next few years. Their actions could increasingly disrupt U.S. critical infrastructure in the health care, financial, government, and emergency service sectors, based on the patterns of activities against these sectors in the last few years."

h. **Insider Threats**. While much of our intelligence is focused on external threats, the U.S. must be aware of threats from within.

(1) In 2010, Army PFC Manning was found not guilty of the most serious charge of knowingly aiding the enemy, but was convicted on 20 other specifications related to the misappropriation of hundreds of thousands of intelligence documents sent to WikiLeaks. Prosecutors alleged that Manning downloaded some 470,000 Significant Activity (SIGACT) reports (from Iraq and Afghanistan) from SIPRNET.

(2) In 2013, Edward J. Snowden, was charged with violations of: Unauthorized Disclosure of National Defense Information; Unauthorized Disclosure of Classified Communication; and Theft of Government Property.

(3) In 2015, a former U.S. Nuclear Regulatory Commission employee pleaded guilty to an attempted spear-phishing cyber-attack on Department of Energy computers to compromise, exploit and damage U.S. government computer systems that contained sensitive nuclear weapon-related information.

Cyberspace Threat Techniques: Adversaries use a myriad of cyberspace techniques to accomplish their objectives. Some of these are:

a. **Brute-Force Attack**. In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account lockout policies allow three to five bad attempts during a set period of time.

(1) **Password-Spray Attack**. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

(2) **Email** applications are also targeted. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud; (2) subsequently download user mail to locally stored email files; (3) identify the entire company's email address list; and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.

b. **Cryptojacking** occurs when malicious cyber actors effectively hijack the processing power of the victim devices and systems by exploiting vulnerabilities – in webpages, software, and operating systems – to illicitly install cryptomining software on victim devices and systems. With the cryptomining software installed, the malicious cyber actors earn cryptocurrency.

(1) **Cryptocurrency** is a digital currency used as a medium of exchange, similar to other currencies. Unlike other currencies, cryptocurrency operates independently of a central bank and uses encryption techniques and blockchain technology to secure and verify transactions.

(2) **Cryptomining** (cryptocurrency mining) is the way in which cryptocurrency is earned. Individuals mine cryptocurrency by using cryptomining software to solve complex mathematical problems involved in

validating transactions. Each solved equation verifies a transaction and earns a reward paid out in the cryptocurrency.

c. **Denial-of-Service (DoS)** is an attack that occurs when a malicious cyber threat actor prevents legitimate users from accessing information systems, devices, or other network resources. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

d. **Distributed Denial-of-Service (DDoS)** attacks occur when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet – a group of hijacked internet-connected devices to carry out large scale attacks.

(1) **Command and Control**. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

(٢) **Botnets** – made up of compromised devices – may also be rented out to other potential attackers. Often the botnet is made available to "attack-for-hire" services, which allow unskilled users to launch DDoS attacks.

(3) **Internet of Things (IoT)**. DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things. IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners' knowledge.

e. **Malicious Code** is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include: viruses, worms, and Trojan horses.

(1) **Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.

(2) **Worms** are a type of virus that self-propagates from computer to computer. Its functionality is to use all of your computer's resources, which can cause your computer to stop responding.

(3) **Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program. It is not uncommon that free software contains a Trojan horse making a user think they are using legitimate software. Instead, the program is performing malicious actions on your computer.

(٤) **Malicious Data Files** are non-executable files – such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file – that exploit weaknesses in the software program used to open it. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing the files via email, social media, and websites.

f. **Ransomware** is a type of malicious software cyber actors use to deny access to systems or data. It is frequently delivered through spearphishing emails and targets critical data and systems for the purpose of extortion. Ransomware often attempts to spread to shared storage drives and other accessible systems. The malicious cyber actor holds systems or data hostage until a ransom is paid. If payment is received, the cyber actor will purportedly provide an avenue for the victim to regain access to the system or data. If the demands are not met, the system or encrypted data remains unavailable, or the data may be deleted.

g. A **Rootkit** is a piece of software that can be installed and hidden on your computer without your knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of a vulnerability on your computer or has convinced you to download it. Rootkits are not necessarily malicious, but they may hide malicious activities. If a Rootkit has been installed, the user may not be aware that their computer has been compromised, and traditional anti-virus software may not be able to detect the malicious programs. Attackers may be able to access information, monitor your actions, modify programs, or perform

other functions on your computer without being detected. Attackers are also creating more sophisticated programs that update themselves so that they are even harder to detect.

h. **Social Engineering Attacks**. An attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

(1) **Phishing** is a form of social engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy organization. Phishing emails are crafted to appear as though they have been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. After the code is run, your computer may become infected with malware.

(2) **Vishing** is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed.

(3) **Smishing** is a form of social engineering that exploits Short Message Service (SMS) or text messages. Text messages can contain links to such things as webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

i. **Spyware** collects information from a computing system without user consent. Spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information. The data is often delivered to online attackers who sell it to others or use it themselves for marketing or spam or to execute financial crimes or identity theft.

(1) **Key Loggers** capture keyboard events and record the keystroke data before it is sent to the intended application for processing. Like most other

spyware capture technologies, software based keyloggers can turn their capture on or off based on keywords or events.

(2) **Network Traffic** is another valuable source of data. Data commonly extracted from network captures includes user names, passwords, email messages, and web content. In some cases, entire files can be extracted and reconstructed from the captured streams.

j. **Wireless Threats**. A wireless-enabled laptop can expose the user to a number of security threats.

(1) **Evil Twin Attacks**. The attacker gathers information about a public access point, then sets up his or her own system to impersonate the real access point. The attacker will use a broadcast signal stronger than the one generated by the real access point. Unsuspecting users will connect using the stronger, bogus signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet.

(2) **Wireless Sniffing**. Many public access points are not secured, and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious users can use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.

(3) **Peer-to-Peer Connections**. Many laptop computers can create ad hoc networks if they are within range of one another. These networks enable computer-to-computer connections. An attacker with a network card configured for ad hoc mode and using the same settings as the victim's computer may gain unauthorized access to sensitive files. An unsecured wireless network combined with unsecured file sharing can spell disaster. Under these conditions, a malicious user could access any directories and files you have allowed for sharing.

Cyberspace Assumptions

1. Commanders and staff should review strategic guidance and direction to see if any assumptions are imposed on the planning process. Where there is insufficient information or guidance, the commander and staff identify assumptions to assist in framing solutions. At this stage, assumptions address strategic and operational gaps that enable the commander to develop the operational approach.

2. **Characteristics of Cyberspace Capabilities**. While cyberspace is complex and ever changing, cyberspace capabilities, whether devices or computer programs, must reliably create the intended effects. However, cyberspace capabilities are developed based on environmental assumptions and expectations about the operating conditions that will be found in the OE.

These conditions may be as simple as the type of computer operating system being used by an adversary or as complex as the exact serial number of the hardware or version of the software installed, what system resources are available, and what other applications are expected to be running (or not running) when the cyberspace capability activates on target. These expected conditions should be well documented by the capability developer and are important for planners and targeting personnel to understand as capability limitations. The extent to which the expected environmental conditions of a target cannot be confirmed through Intelligence, Surveillance and Reconnaissance (ISR) sources represents an increased level of risk associated with using the capability. All other factors being equal, cyberspace capabilities that have the fewest environmental dependencies and/or allow the operator to reconfigure the capability are preferred.

Cyberspace Actions and the Operational Approach

1. The operational approach is a commander's description of the broad actions the force can take to achieve an objective in support of the national objective or attain a military end state. It provides the foundation for the commander's planning guidance to the staff and other partners by providing the commander's visualization of how the joint force's operations will transform current conditions into the desired conditions – the way the commander envisions the OE at the conclusion of operations to support national objectives. The operational approach is based largely on an understanding of the OE and the problem facing the commander.

2. **Operations *'In'*, *'Through'*, and *'External'* to Cyberspace**. When developing an operational approach, commanders should synchronize actions '*in*' and '*through'* cyberspace with other activities to achieve the desired objectives. Actions '*in*' cyberspace are typically offensive and defensive operations that deny an adversary's use of resources or manipulate an adversary's information, information systems, or networks. On the other hand, the military operates '*through'* cyberspace on a routine basis as it conducts joint functions: command and control, intelligence, fires, movement and maneuver, protection, sustainment, and information. These

joint functions comprise related capabilities and activities grouped together to help commanders integrate, synchronize, and direct operations (see Figure 2).

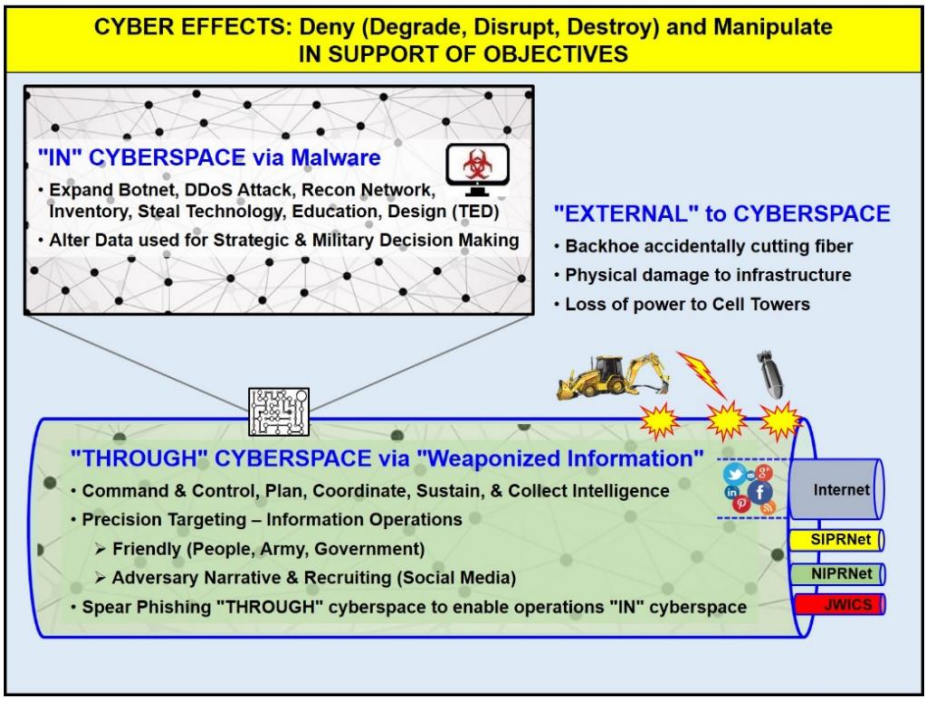

Figure 2: Operations In, Through, and External to Cyberspace

3. **U.S. Military Dependence on Cyberspace**. Commanders must be aware that U.S. military forces are critically dependent on networks and information systems to conduct operations. Nearly every conceivable component within DOD is networked. These networked systems and components are inextricably linked to the Department's ability to project military force and the associated mission assurance. Over the past decades, DOD developed its Full Spectrum Dominance doctrine that envisioned information superiority to great advantage as a force multiplier. The power of this doctrine and its near total reliance on information superiority led to networking almost every conceivable component within DOD, with frequent networking across the rest of government, commercial and private entities, and coalition partners in complex, intertwined paths. While proving incredibly beneficial, these ubiquitous IT capabilities have also made the United States increasingly dependent upon safe, secure access and the integrity of the data contained in the networks. A weakness of the implementation of this doctrine is its focus on functionality, connectivity, and cost of information superiority over security – similar to the development of the Internet.

4. **Cyberspace Vulnerabilities**. The performance of U.S. military forces has demonstrated the superiority of networked systems coupled with kinetic capabilities and well-trained forces. Adversaries have discovered that the same connectivity and automation that provides great advantage to the United States, is also a weakness that presents an opportunity to undermine U.S. capabilities in a very asymmetric way. The network attack tools that are available on the commercial market are available to our adversaries. In addition, adversaries with financial means will invest to improve those tools and build more capable weapons to attack U.S. military systems and national infrastructure.

5. **Cyberspace Missions**. All actions in cyberspace that are not simply cyberspace-enabled activities are taken as part of one of three cyberspace missions: DODIN operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO). Cyberspace Operations can contribute directly to the commander's visualization of the operational approach and achievement of desired effects, conditions, and end state objectives. The successful execution of CO requires integration and synchronization of these missions.

a. **DOD Information Network (DODIN) Operations**. The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN. These include proactive cyberspace security actions which address vulnerabilities of the DODIN or specific segments of the DODIN. DODIN operations are network-focused and threat-agnostic: the cyberspace forces and workforce undertaking this mission endeavor to keep all threats out of a particular network or system they are assigned to protect. DODIN operations is a standing mission, and although many DODIN operations activities are regularly scheduled events, they cannot be considered routine, since their aggregate effect establishes the framework on which most DOD missions ultimately depend.

b. **Defensive Cyberspace Operations (DCO)**. DCO missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace. Specifically, they are missions intended to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. This distinguishes DCO missions, which defeat specific threats that have bypassed, breached, or are

threatening to breach security measures, from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any specific threat activity. DCO are threat-specific and frequently support mission assurance objectives. DCO missions are conducted in response to specific threats of attack, exploitation, or other effects of malicious cyberspace activity and leverage information from maneuver, intelligence collection, counterintelligence (CI), law enforcement (LE), and other sources as required. DCO include outmaneuvering or interdicting adversaries taking or about to take actions against defended cyberspace elements, or otherwise responding to imminent internal and external cyberspace threats. The goal of DCO is to defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state.

c. **Offensive Cyberspace Operations (OCO)**. OCO are CO missions intended to project power in and through foreign cyberspace through actions taken in support of Combatant Commander (CCDR) or national objectives. OCO may exclusively target adversary cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, etc. All CO missions conducted outside of blue cyberspace with a commander's intent other than to defend blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions. Like DCO-RA missions, some OCO missions may include actions that rise to the level of use of force, with physical damage or destruction of enemy systems. Specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities and national policy considerations. OCO missions require a properly coordinated military order and careful consideration of scope, ROE, and measurable objectives.

6. **Cyberspace Actions**. Execution of any OCO, DCO, or DODIN operations mission requires completion of specific tactical-level actions or tasks that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of these actions, which are defined exclusively by the types of effects they create. To plan for, authorize, and assess these actions, it is important the commander and staff clearly understand which actions have been authorized under their current mission order. Since they will always be necessary, standing orders for DODIN operations and DCO-IDM missions cover most cyberspace security and initial cyberspace defense actions. However, OCO and DCO-RA missions are episodic. They may require clandestine maneuver and collection actions or may require overt actions, including fires.

Therefore, the approval for CO actions in foreign cyberspace requires separate OCO or DCO-RA mission authorities. The cyberspace actions are:

a. **Cyberspace Security**. Cyberspace security actions are taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other IT, including PIT, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Although they are threat-informed, cyberspace security actions occur in advance of a specific security compromise and are a primary component action of the DODIN operations mission. Cyberspace security actions protect from threats within cyberspace by reducing or eliminating vulnerabilities that may be exploited by an adversary and/or implementing measures to detect malicious cyberspace activities.

b. **Cyberspace Defense**. Cyberspace defense actions are taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach the cyberspace security measures and include actions to detect, characterize, counter, and mitigate threats, including malware or the unauthorized activities of users, and to restore the system to a secure configuration. The Combatant Command (CCMD), Service, or DOD agency that owns or operates the network is generally authorized to take these defensive actions except in cases when they would compromise the operations of elements of cyberspace outside the responsibility of the respective CCMD, Service, or agency.

c. **Cyberspace Exploitation**. Cyberspace exploitation actions include military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation actions are taken as part of an OCO or DCO-RA mission and include all actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions. Cyberspace exploitation also supports current and future operations through collection of information, including mapping red and gray cyberspace to support situational awareness; discovering vulnerabilities; enabling target development; and supporting the planning, execution, and assessment of

military operations. Cyberspace exploitation actions are deconflicted with other USG departments and agencies in accordance with national policy.

d. **Cyberspace Attack**. Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial effects in the physical domains. Unlike cyberspace exploitation actions, which are often intended to remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality. Cyberspace attack actions are a form of fires, are taken as part of an OCO or DCO-RA mission, are coordinated with other USG departments and agencies, and are carefully synchronized with planned fires in the physical domains.