Detect, Deny, Degrade, Disrupt, Destroy, Deceive: Which is the Greatest in OCO?

Tim Grant
R-BAR, Benschop, The Netherlands

tim.grant.work@gmail.com

Abstract: In the cyber kill chain literature, possible courses of action are listed as *detect*, *deny*, *degrade*, *disrupt*, *destroy*, and *deceive* (a.k.a. "the 6Ds"). These verbs denote defensive action to be taken against an intruder. By comparison, military doctrine for cyberspace operations encompasses cyberspace exploitation and attack, as well as defence. The question arises whether the 6Ds are also applicable to offensive action, i.e. exploitation and attack, or whether additional action verbs are needed. Military doctrine is evolving towards all-domain operations, in which action in cyberspace is integrated with action in the physical domains of land, sea, air, and space. This prompts the question as to whether the 6Ds are also suited to action in a physical domain. A pilot study of actual military operations that integrated cyber and physical action suggests that deception, delay, and denial of organisational and cyber entities is suited to cyber action, while seizure, capture, and destruction of physical entities is suited to physical action. Preference among action verbs may indicate when it is best to engage targets using cyber or physical resources and which action is preferred. This paper identifies which action verbs are best suited to offensive cyber operations in the context of all-domain operations. The paper reviews related theory on cyberspace and the cyber kill chain. It identifies action verbs in US Department of Defense (DoD) doctrine on information and cyberspace operations, comparing them to those in the US DoD Dictionary of Military and Associated Terms. After discussing the findings, the paper draws conclusions and recommends further work.

Keywords: Action verbs, strategic effects, offensive cyber operations, computer network attack, all-domain operations.

1. Introduction

1.1 Motivation

The cyber kill chain approach (Croom, 2010) introduced a proactive strategy for defending computer-based systems from intrusion. By focusing on the threat element of risk (namely the attacker), rather than on the system's vulnerabilities, the defender can cut off the attack before it has achieved its goals. This makes it possible to defend against intrusive attacks in real time and, in particular, against Advanced Persistent Threats (APTs).

The approach centres on the sequence of phases that an attacker must pass through to achieve his/her objectives (Croom, 2010): *reconnaissance*, *weaponization*, *delivery*, *exploitation*, *installation*, *command and control*, and *actions on objectives*. This sequence is the attacker's *kill chain*. The defender can interrupt the kill chain in any phase by taking appropriate action. Hutchins, Cloppert & Amin (2011, p.117) categorize the defender's possible courses of action as *detect*, *deny*, *degrade*, *disrupt*, *destroy*, and *deceive* (a.k.a. "the 6Ds").

In this paper, we focus on the attacker's viewpoint. The question then arises as to whether the 6Ds completely describe an intruder's possible courses of action. Military doctrine assumes that some or all of the 6Ds apply to offensive cyber operations (OCO), covering both exploitation (a.k.a. intelligence gathering and analysis, manoeuvre, and enabling actions) and attack. For example, US cyberspace operations doctrine identifies *deny*, *degrade*, *disrupt*, *destroy*, and *manipulate* as actions that can be taken in cyberspace attack (US DoD, 2018, p.II-7). More widely, the US Department of Defense (DoD) Dictionary of Military and Associated Terms (US DoD, 2021, p.2) lists 32 strategic effects that denote all possible military actions. This begs the question as to how many of these verbs are applicable to the cyberspace domain and which are applicable only to the physical domains (land, sea, air, and space). The answer is important for targeting, especially in all-domain operations (ADO) where the right military asset and the right action must be chosen to engage a target in any of the five domains (Borne, 2019).

A pilot study (Grant & Kantola, 2021) of actual military operations that integrated cyber and physical ("kinetic") actions in an offensive operation suggests that cyber action is suited to deception, delay, and denial of organisational and cyber entities, such as military units, user accounts, and stored data. By contrast, kinetic action is suited to the seizure, capture, and destruction of physical entities, such as territory, buildings, and equipment. It is noteworthy that this pilot study already identified three verbs (*delay*, *seize*, and *capture*) not listed in the 6Ds. These suggestive results need to be checked against OCO-related doctrine.

1.2 Purpose, scope, and paper structure

The purpose of this paper is to identify which action verbs are best suited to OCO in the context of ADO, where OCO includes both computer network exploitation and computer network attack. It contributes to meeting Lin's (2009) and Denning & Denning's (2010) calls for an open discussion of OCO in the scientific literature. The focus is on OCO performed by professional military and law enforcement organisations at the operational and tactical levels. It assumes that the operation is aimed at penetration of the target system(s).

This paper contains six sections. After an introductory section, Section 2 reviews related theory on cyberspace and the cyber kill chain. Section 3 reviews the relevant US military doctrine. Section 4 maps the action verbs found in the doctrinal publications to the 32 verbs from the US DoD Dictionary of Military and Associated Terms. Section 5 discusses the findings, and Section 6 draws conclusions and recommends further work.

2. Related Theory

2.1 Cyberspace

The US DoD defines cyberspace as the part of the information environment consisting of the interdependent network of ICT infrastructures and data (US DoD, 2018). It includes the Internet, communications networks, computer systems, embedded processors and controllers, and the information residing in and passing through these networks and systems. Cyberspace operations are the employment of cyberspace capabilities aimed at achieving objectives in or through cyberspace, and may be defensive or offensive in nature.

In military doctrine, cyberspace is typically modelled as a set of distinct, yet interrelated layers. We adopt UK doctrine because this covers both physical and cyber domains, as needed in ADO. There are six layers (UK MoD, 2016): *social*, *people*, *persona*, *information*, *network*, and *real*, with the real layer being divided into *physical* and *geographical* aspects.

Table 1: Layers in physical and cyber domains (adapted from UK MoD, 2016).

Layer	Entities found in this layer	Domain
Social	Organisations, groups & teams; human-human interaction; processes & SOPs; organisational culture.	Physical
People	Individuals (users, developers, administrators, maintainers).	
Persona	Accounts (user, e-mail, etc).	Cyber
Information	Data, applications & protocols; domain names; logical connections between nodes.	
Network	Network nodes and links.	
Real (with 2 aspects): - Physical - Geographical	Infrastructure; buildings; devices; cables; wireless & optical communication links. Locations of infrastructure, devices, cables, & communication links, and of individuals, groups, teams & organisations.	Physical

Inter-entity relationships often cross layers and may combine physical and cyber domains. For example, accounts (*persona* layer) are owned by individuals (*people* layer). Manned weapon systems, such as armoured vehicles, ships, or aircraft, carry teams (*social* layer) of individuals (*people* layer), are constructed from physical devices (*real* layer, *physical* aspect), and can be found at a geographical location (*real* layer, *geographical* aspect). They can be fitted with Command & Control (C2) and communications systems consisting of hardware (*real* layer, *physical* aspect) and software plus data (*information* layer) connected in a network (*network* layer), with login accounts (*persona* layer) for the individuals. Moreover, in sensor and weapon control systems and in C2 systems, data (a cyber entity in the *information* layer) may represent or stand in for entities in the physical domain. For example, data in a C2 system may represent a real-world aircraft, with its identity and type, its geographical location, altitude, speed, and direction of travel, and whether it is hostile, friendly, or neutral.

2.2 Cyber kill chain

The term *kill chain* is a military concept describing the attack process (irrespective of which domain(s) it occurs in) as a chain of actions. If any link in the chain is broken, then the attack fails. Lockheed Martin applied the concept to defending computer-based systems in Croom (2010). The cyber kill chain is detailed in Table 2.

Table 2: The components of the cyber kill chain (Croom, 2010, p.54).

Phase	Description
Reconnaissance	Research, identification and selection of targets, often represented as crawling Internet Web sites looking for email addresses or information on specific technologies.
Weaponization	Coupling a remote access Trojan with an exploit into a deliverable payload, typically using an automated tool. Increasingly, data files such as Microsoft Office documents or Adobe PDF files serve as the weapon delivery device.
Delivery	Transmission of the weapon to the target. The three most prevalent delivery vectors for weaponized payloads are e-mail, Web sites, and USB removable media.
Exploitation	Triggering of the attacker's code. Most often, the weapon exploits an application or operating system vulnerability. It might simply exploit the user persuading him to open an executable attachment, or leverage a feature of the operating system that auto-executes code.
Installation	Installing a remote access Trojan or backdoor on the victimized system, allowing the attackers to affect all users of the system and to maintain persistence across system reboots.
C2	Accomplished most often with an outbound beacon to an Internet controller server, which establishes the C2 channel. This connection provides the manual "hands-on-the-keyboard" access that is required by most APT malware.
Actions on objectives	The final stage required for a successful intrusion. The most common objective is data exfiltration: collecting, encrypting, and stealing information from the compromised system. Attackers might also seek to violate data integrity or availability. Yet another objective might be to move laterally through the victim's IT environment, spawning new kill chains on subsequent targets.

Hutchins, Cloppert & Amin (2011) described in detail the Lockheed Martin model for the cyber kill chain and its application to cyber defence, particularly against campaigns of multiple attacks (as would occur with APTs). It introduced the defender's courses of action, listed as the verbs *detect*, *deny*, *disrupt*, *degrade*, *deceive*, and *destroy* (a.k.a. "the 6Ds"). Hutchins et al did not define the 6Ds.

Hutchins et al (2011) related the 6Ds to cyber kill chain phases in the form of a matrix; see Table 3. The abbreviations are explained follows (ibid., p.117): "*This matrix depicts in the exploitation phase, for example, that host intrusion detection systems (HIDS) can passively detect exploits, patching denies exploitation altogether, and data execution prevention (DEP) can disrupt the exploit once it initiates. Illustrating the spectrum of capabilities defenders can employ, the matrix includes traditional systems like network intrusion detection systems (NIDS) and firewall access control lists (ACL), system hardening best practices like audit logging, but also vigilant users who can detect suspicious activity.*"

Table 3: Courses of action matrix (Hutchins et al, 2011, Table 1, p.117).

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on objectives	Audit log			Quality of service	Honeypot	

There have been criticisms of the Lockheed Martin model of the cyber kill chain, but these criticisms are irrelevant to this paper.

3. Relevant doctrine

Doctrine is as important to (military) practitioners as theory is to scientists. Military doctrine expresses the military's institutional culture, the way it fights, and its relationship with the society and state that sustains it (Jackson, 2013).

We restrict our research to US DoD doctrine. The authoritative public-domain source for current doctrinal publications is the US Joint Chiefs of Staff Doctrine website (https://www.jcs.mil/Doctrine/). We found action verbs in doctrine on information operations (IO), cyberspace operations (CO), and countering threat networks (CTN). No US DoD doctrine has been published for ADO.

3.1 Information operations

Hutchins et al (2011, p.5) explicitly states that the 6Ds came from the 2006 version of Joint Publication (JP) 3-13 *Information Operations* (US DoD, 2006). This version not only includes the 6Ds but also five additional verbs: *exploit*, *influence*, *protect*, *restore*, and *respond*. Hutchins et al do not explain why they excluded the additional verbs, despite most of them being obviously applicable to CO. All 11 verbs are defined as shown in Table 4.

Table 4: Actions defined in JP 3-13 (US DoD, 2006), p.I-9 & I-10.

Action	Definition
Destroy	To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
Disrupt	To break or interrupt the flow of information.
Degrade	To reduce the effectiveness or efficiency of adversary C2 or communication systems, and information collection efforts or means. Information operations can also degrade the morale of a unit, reduce the target's worth or value, or reduce the quality of adversary decisions and actions.
Deny	To present the adversary from accessing and using critical information, systems, and services.
Deceive	To cause a person to believe what is not true. Military deception seeks to mislead adversary decision makers by manipulating their perception of reality.
Exploit	To gain access to adversary C2 systems to collect information or to plant false or misleading information.
Influence	To cause others to behave in a manner favourable to own forces.
Protect	To take action to guard against espionage or capture of sensitive equipment and information.
Detect	To discover or discern the existence, presence, or fact of an intrusion into information systems.
Restore	To bring information and information systems back to their original state.
Respond	To react quickly to an adversary's or others' information operations attack or intrusion.

JP 3-13 was subsequently updated in 2012 and 2014, but no action verbs appear in these later versions. Instead, readers are referred to JP 3-12 for details on CO. This is because CO – then termed *computer network operations* – were included in IO in 2006. Around 2010, CO was split off from IO when US Cyber Command was established (Theohary, 2022).

More recently, the doctrinal emphasis has shifted to the generation and use of information in joint operations. In September 2022, JP 3-13 was replaced by JP 3-04 *Information in Joint Operations*, but this document is not available to the public (Pomerleau, 2022).

3.2 Cyberspace operations

The first version of JP 3-12 *Cyberspace Operations* was published in 2013, but was classified. An unclassified update was published in 2018, and this is the version used in this paper (US DoD, 2018). JP 3-12 has since been updated in January 2022, but this version is not available to the public.

JP 3-12 (US DoD, 2018) has four chapters. Chapter 1 is introductory, outlining the nature of cyberspace and setting the framework for using cyberspace forces and capabilities. Chapter 2 is most relevant to this paper as it describes the core activities in CO. Action verbs are mentioned only in the context of OCO. By contrast, Chapters 3 and 4 describe the US-specific CO organisation and procedures, and are therefore not relevant.

JP 3-12 identifies three main cyberspace missions: operating the US DoD's own ICT infrastructure ("blue" cyberspace), and defensive and offensive CO. OCO are missions intended to project power in and through foreign cyberspace. Foreign cyberspace may be "red", denoting cyberspace controlled by the adversary, or "grey", meaning neutral cyberspace that is neither blue nor red. OCO targets adversary cyberspace functions or creates first-order cyber effects that cascade into the physical domains. Offensive actions may rise to the level of the use of force, up to physical damage to or destruction of the adversary's systems.

There are two types of offensive cyber action: exploitation and attack. Cyberspace exploitation is often clandestine and includes military intelligence, manoeuvre, information collection, and other enabling actions in preparation for future operations. In other words, it covers intelligence, surveillance and reconnaissance (ISR), espionage, and the planting of APTs. By contrast, cyberspace attack creates noticeable denial effects in cyberspace or manipulates red cyberspace so as to create denial effects in the physical domains. Action verbs define these denial effects, as shown in Table 5.

Table 5. Actions defined in JP 3-12 (US DoD, 2018), p.II-7.

Action	Definition
Deny	To prevent access to, operation of, or availability of a target function by a specified level for a specified time. Deny is sub-divided into Degrade, Disrupt, and Destroy.
Degrade	To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified.
Disrupt	To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent.
Destroy	To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.
Manipulate	Manipulation, as a form of cyberspace attack, controls or changes information, information systems, and/or networks in grey or red cyberspace to create physical denial effects, using deception, decoying, conditioning, spoofing, falsification, and other similar techniques. It uses an adversary's information resources for friendly purposes, to create denial effects not immediately apparent in cyberspace. The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence of the logical first-order effect.

3.3 Countering threat networks

Since the targets of OCO will invariably be networks, we also considered JP 3-25 *Countering Threat Networks* (US DoD, 2016). In JP 3-25, threat networks are organisational networks, such as the organisational structure of and communication flow in terrorist and criminal organisations. Threat networks can be engaged using both physical and cyber action. Since action verbs were found in JP 3-25, we included the publication in our analysis.

JP 3-25 (US DoD, 2016) has six chapters. Chapter 5 is most relevant to this paper because it describes the activities required to counter threat networks, including the desired effects (a.k.a. action verbs). The other chapters are not relevant, describing threat networks (Chapters 1 and 2), their environment (Chapter 3), and how to plan operations to counter them (Chapter 4), and how to assess the results (Chapter 6).

There are four strategies for countering threat networks. The counter-resource strategy progressively weakens the threat's ability to conduct operations. The decapitation strategy removes leadership nodes within the network. The fragmentation strategy surgically removes key communication nodes within the network so as to disrupt its ability to function. Finally, the counter-messaging strategy projects messages designed to discourage the recruitment of new members to the threat network and to encourage existing members to leave the network.

The desired effects are selected based on the commander's vision on the future conditions for the threat network and its environment. Action verbs and their definitions are shown in Table 6.

Table 6. Actions defined in JP 3-25 (US DoD, 2016), p.V-4 to V-8.

Action	Definition
Neutralise	To render enemy personnel or materiel incapable of interfering with a friendly operation. Neutralisation of an entire network may not be feasible, but through analysis the commander's staff has the ability to identify key parts to target that will neutralise specific functions.
Degrade	To reduce the effectiveness of efficiency of the threat network by eliminating critical capabilities of the network.
Disrupt	To upset an enemy's formation or tempo, to interrupt the enemy's timetable, or to cause the enemy to commit prematurely or attack in a piecemeal fashion. Should disruption result in the elimination of nodes, the staff must also consider the network's means and time necessary to reconstitute.
Destroy	To physically render an enemy force combat ineffective until it is reconstituted. Alternatively, to damage the enemy so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
Defeat	To affect the threat network to the extent that it has temporarily or permanently lost the physical means or the will to fight.
Deny	To hinder or deny the enemy the use of territory, personnel, or facilities by destruction, removal, contamination, or obstruction.
Divert	To draw the threat network's attention and forces away from a friendly operation by means of attack, alarm, or feint. Diversions can also cause more circuitous routing, resulting in delays for enemy forces.

4. Analysis

The purpose of this section is to compare the action verbs found in the US DoD doctrine publications with the 6Ds and then to map them to the action verbs found in the US DoD Dictionary.

4.1 Comparing action verbs in doctrine with 6Ds

First, in Table 7 we compare the action verbs obtained from the doctrine publications against the 6Ds. The action verbs are listed top to bottom in alphabetical order.

Table 7. Comparing action verbs with 6Ds.

Cyber kill chain (6Ds)	IO (JP 3-13)	CO (JP 3-12)	CTN (JP 3-25)
Deceive	Deceive	(Deceive – see Manipulate)	
			Defeat
Degrade	Degrade	Degrade	Degrade
Deny	Deny	Deny	Deny
Destroy	Destroy	Destroy	Destroy
Detect	Detect		
Disrupt	Disrupt	Disrupt	Disrupt
			Divert
	Exploit		
	Influence		
		Manipulate (Using deception, decoying, conditioning, spoofing, and falsification)	
			Neutralise
	Protect		
	Respond		
	Restore		

This comparison suggests that the action verbs *degrade*, *deny*, *destroy*, and *disrupt* are common across all three doctrine publications. However, the definitions of the action verbs differ. This is because the intended targets have differing characteristics. In IO, the targets are people's minds, i.e. entities in the *people* layer. In CO, the targets are ICT infrastructure and data, i.e. entities in the *real* / *physical* layer (e.g. hardware), *network* layer, *information* layer (software and data), and possibly *persona* layer (accounts). In CTN, the targets are organisations (in the *social* layer), members and potential members (in the *people* layer), and their communication structures (in the *information* and *network* layers).

4.2 Mapping to verbs in US DoD Dictionary

One way of resolving the differences in definitions is to map the action verbs to those listed in the US DoD Dictionary. Like JP 3-12 and JP 3-04, the latest version (November 2022) of this Dictionary is not currently available on the US Chiefs of Staff Doctrine website. A search of the Internet showed that the most up-to-date version (November 2021) could be found on the Federation of American Scientists' website (US DoD, 2021). This version lists the action verbs as follows (ibid., p.2):

> *"The following is a lengthy but not whole inclusive list of strategic effect terms: advance, assure, coerce, compete, compel, contain, deceive, defeat, degrade, delay, delegitimize, deny, destroy, deter, discredit, disable, discourage, disrupt, divert, engage, enhance, integrate, isolate, kill, maintain, manage, neutralize, prevent, protect, stabilize, suppress, synchronize."*

Unfortunately, only one of these 32 verbs (*neutralize*) is defined in the DoD Dictionary. Moreover, there were 11 more verbs in the pilot study and the doctrine publications. Since the DoD Dictionary states (US DoD, 2021, p.2): "*For strategic effect terms, the standard dictionary definition often applies"*, we decided to follow this suggestion for all 43 verbs. For convenience, we chose the online Collins English dictionary (https://www.collinsdictionary.com/dictionary/english).

The full list was too unwieldy for our research. We observed that several verbs described action on a situation or condition, rather than action on an entity (such as those listed in Table 1). In addition, there were several verbs that could be regarded as synonyms. After pruning, the resulting action verbs, together with their source, any synonyms, and the definition selected from the Collins English dictionary, are listed in Table 8. The original 6Ds are underlined.

Table 8. Action verbs resulting from mapping to DoD Dictionary definitions (6Ds underlined).

Verb	Source(s)	Synonym(s)	Definition (Collins)
coerce	Dictionary, JP 3-13, JP 3-12	compel, deter, discourage, influence, condition	2. If you coerce someone into doing something, you make them do it, although they do not want to.
deceive	Dictionary, 6Ds, JP 3-12	decoy, spoof, falsify	If you deceive someone, you make them believe something that is not true, usually in order to get some advantage for yourself.
degrade	Dictionary, 6Ds		2. To degrade something means to cause it to get worse.
delay	Dictionary, pilot	latency	2. To delay someone or something means to make them late or to slow them down.
deny	Dictionary, 6Ds, JP 3-13	contain, isolate, prevent, protect, suppress	3. If you deny someone something that they need or want, you refuse to let them have it.
destroy	Dictionary, 6Ds	kill	1. To destroy something means to cause so much damage to it that it is completely ruined or does not exist anymore.
detect	6Ds		1. To detect something means to find it or discover that it is present somewhere by using equipment or making an investigation. 2. If you detect something, you notice it or sense it, even though it is not very obvious.
disrupt	Dictionary, 6Ds	disable, neutralize	If someone or something disrupts an event, system, or process, they cause difficulties that prevent it from continuing or operating in a normal way.
divert	Dictionary, JP 3-25		1. To divert vehicles or travellers means to make them follow a different route or go to a different destination than they originally intended.
exploit	JP 3-13	manipulate	3. If you exploit something, you use it well, and achieve something or gain an advantage from it.
identify	(See text)	recognize, classify	1. If you can identify someone or something, you are able to recognize them or distinguish them from others.
integrate	Dictionary		3. If you integrate one thing with another, or one thing integrates with another, the two things become closely linked or form part of a whole idea or system.
move	Dictionary	advance	2. When you move, you change your position or go to a different place.
observe	(See text)	Monitor, survey	1. If you observe a person or thing, you watch them carefully, especially in order to learn something about them.
penetrate	(See text)		1. If something or someone penetrates a physical object or an area, they succeed in getting into it or passing through it.
respond	JP 3-13	react	1. When you respond to something that is done or said, you react to it by doing or saying something yourself.
restore	Dictionary, JP 3-13	maintain	2. To restore someone or something to a previous condition means to cause them to be in that condition once again.
seize	pilot	capture	3. If a government or other authority seize someone's property, they take it from them, often by force.
synchronize	Dictionary		If you synchronize two activities, processes, or movements, or if you synchronize one activity, process, or movement with another, you cause them to happen at the same time and speed as each other.

The author's choice of definitions, of which verbs to retain, and of which to regard as synonyms is unavoidably subjective. Some verbs require explanation, as follows:

- *Observe* and *identify*. Neither the doctrine publications nor the DoD Dictionary include terms that describe the ISR process. The 6Ds only hint at ISR in the guise of *detect*. Detection of potential targets occurs as a result of observing an area, and after detection the target is identified as an instance of a particular entity and classified as friendly, hostile, or neutral.
- *Move*. The first term in the DoD Dictionary list is *advance*, but there are no other terms denoting movement in physical or cyber space. We considered the term *manoeuvre*, but rejected this because it is a more complex concept.
- *Penetrate*. In OCO, penetration of the target system is a key step in the attack process. In effect, penetrate is overcoming the defender's *deny* (a.k.a. *protect*) action.
- *Seize*. The term *seize*, together with its synonym *capture*, was identified in the pilot study. Although it was only used for the physical domain, the verb is equally applicable to taking (over) control of cyber entities.
- *Respond*. The majority of action verbs found are proactive in nature. Even so, some actions will be a reaction to the defender's actions. We adopted the verb *respond* from JP 3-13.

5. Findings

While comparing the action verbs and mapping them to the verbs in the DoD Dictionary, we observed a number of conceptual shortcomings in the 6Ds. The lack of verbs fully describing the ISR process has already been mentioned. Other shortcomings are as follows:

- *Space, location, distance, and movement*. The 6Ds lack concepts of location, of distance between locations, and of movement. Both physical and cyber action take place in a space. Physical space is continuous and has three dimensions. Cyberspace is discrete and multi-dimensional. For example, an important aspect of OCO is gaining access to the target system (Anon & Anon, 2022), The access path may cross both physical and cyber space (cf. over an air-gap, as in Stuxnet).
- *Time, duration, and synchronization*. The need to add the action verbs *delay* and *synchronize* show that the 6Ds lack concepts of time, duration, and synchronization.
- *Control over entities*. The need to add the action verb *seize* showed that the 6Ds lacked the concept of the ownership or control over entities.
- *Aggregation and disaggregation of entities*. The action verb *integrate* from the DoD Dictionary describes aggregating several individual entities to become a single compound entity. The reverse process splits a compound entity into its constituent entities. The 6Ds do not cover these concepts.

In summary, the 19 action verbs listed in Table 8 can be grouped into the following categories:

- Spatial verbs: *divert*, *move*.
- Temporal verbs: *delay*, *synchronize*.
- ISR verbs: *detect*, *identify*, *observe*.
- Entity aggregation verbs: *integrate*.
- Entity control verbs: *seize*.
- Effects on targets: *coerce*, *deceive*, *degrade*, *deny*, *destroy*, *disrupt*, *exploit*, *penetrate*, *respond*, *restore*.

Finally, we can answer the questions we set ourselves, as follows:

- Are the 6Ds applicable to OCO? Yes, as demonstrated by JP 3-12.
- Are some verbs preferred for cyber action and others for kinetic action? No, we found no evidence for preferences. All the verbs in Table 8 can be applied equally well to physical and cyber entities, perhaps using synonyms (e.g. *pivot* for *move)*.
- Which is the greatest of the 6Ds? No evidence could be found for any one being the greatest.

6. Conclusions and Further Research

The cyber kill chain approach (Croom, 2010) introduced a proactive strategy for defending computer-based systems from intrusion. The defender can interrupt the intruder's kill chain in any phase by taking appropriate action. Drawing on US Department of Defense doctrine for information operations, Hutchins, Cloppert & Amin (2011) identified the defender's possible actions as *detect*, *deny*, *degrade*, *disrupt*, *destroy*, and *deceive* (a.k.a. "the 6Ds").

This paper identifies which action verbs are best suited to OCO in the context of all-domain operations (ADO). The focus is on action by professional organisations at the operational and tactical levels. A pilot study (Grant & Kantola, 2021) suggested that *deceive*, *delay*, and *deny* were suited to cyber action and *seize*, *capture*, and *destroy* to physical action. It identified more verbs than the 6Ds.

The 6Ds were traced back to the 2006 version of the US DoD Joint Publication (JP) 3-13 *Information Operations*. This publication included yet more verbs. When cyberspace operations were split off from information operations around 2010, separate doctrine was published as JP 3-12 *Cyberspace Operations*. This document included five of the 6Ds, solely in OCO. Four of the 6Ds were also found in JP 3-25 *Countering Threat Networks*. These observations confirmed that the 6Ds were applicable to OCO as well as defence.

All the action verbs found were mapped to the 32 strategic effect terms found in the US DoD Dictionary of Military and Associated Terms. After pruning out synonyms and action on situations, the remaining verbs exhibited shortcomings in that they lacked any representation of space, time, ISR, and entity control and aggregation. Rectifying these shortcomings yielded a set of 19 action verbs for which definitions were obtained from the Collins English dictionary. All 19 could be applied to both cyber and physical action.

The main contribution of this paper is that it harmonizes action verbs from a variety of OCO-related doctrine publications with definitions from a standard English dictionary. In doing so, it rectifies shortcomings, groups them into categories, and shows that all verbs are applicable to ADO. The main limitation is that the choice of definitions and of which verbs to retain is subjective.

Further work is needed to relate the action verbs to attack phases (as in Table 3) and to entities in the six layers of physical and cyber space (see Table 1). Moreover, it may be possible to identify common sequences of action verbs (e.g. *move*, *observe*, *detect*, *identify*, *exploit*), together with the entities involved. More fundamentally, theory and doctrine could be linked by revisiting older work on deriving action verbs from Boisot's model of data, information, and knowledge (Hutchinson & Warren, 2001) and from the Shannon-Weaver model of communications and hypergame theory (Kopp, 2003).

References

Anon & Anon. (2022) All About Access: Inzichten en implicaties van MIVD-cyberoperaties voor digitale slagkracht. *Militaire Spectator*, 191, 9, 464-475. [In Dutch: All About Access: Insights and implications of MIVD cyber operations for digital fighting power.]

Borne, D. (2019). Targeting in Multi-Domain Operations. *Military Review*, May-June, 60-67.

Croom, C. (2010). The Cyber Kill Chain: A foundation for a new cyber security strategy. *High Frontier: The journal for space and cyberspace professionals*, 6, 4, 52-56, August 2010, US Air Force Space Command.

Denning, P.J. & Denning, D.E. (2010). Discussing cyber attack. *Communications of the ACM*, 53, 9, 29-31.

Grant, T.J. and Kantola, H. (2021). Targeting in All-Domain Operations: choosing between cyber and kinetic action. Proceedings, 20th European Conference on Cyber Warfare and Security, 24-25 June 2021, 139-148.

Hutchins, E., Cloppert, M. & Amin, R. (2011). Intelligence-driven Computer Network Defense informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings, 6th International Conference of Information Warfare, 17-18 March 2011, 113-125.

Hutchinson, W. & Warren, M. (2001). *Information Warfare: Corporate attack and defense in a digital world*. Routledge, Abingdon, UK.

Jackson, A.P. (2013). *The Roots of Military Doctrine: Change and continuity in understanding the practice of warfare*. Combat Studies Institute Press, Fort Leavenworth, Kansas, US.

Kopp, C., 2003. Shannon, hypergames and information warfare. *Journal of Information Warfare*, *2*(2), 108-118.

Lin, H. (2009). Lifting the veil on cyber offense. *IEEE Security & Privacy*, 7, 4, 15-21.

Pomerleau, M. (2022). DOD publishes revised doctrine on information. 7 October 2022, DefenseScoop, https://defensescoop.com/2022/10/07/dod-publishes-revised-doctrine-on-information/ (accessed 26 October 2022).

Theohary, C.A. (2022). Defense Primer: Information Operations, In Focus, Library of Congress, Congressional Research Services report IF10771, version 9, 9 December 2022.

UK MoD. (2016). *Cyber Primer*. 2nd edition, Development, Concepts & Doctrine Centre, MoD Shrivenham, UK, July 2016.

US DoD. (2006). *Information Operations*. US DoD Joint Publication 3-13, 13 February 2006.

US DoD. (2016). *Countering Threat Networks*. US DoD Joint Publication 3-25, 21 December 2016.

US DoD. (2018). *Cyberspace Operations*. US DoD Joint Publication 3-12, 8 June 2018.

US DoD. (2021). *US DoD Dictionary of Military and Associated Terms*. November 2021. https://irp.fas.org/doddir/dod/dictionary.pdf (accessed 17 December 2022).