Handbook for Tactical Operations in the Information Environment

Online Appendixes

MICHAEL SCHWILLE, JONATHAN WELCH, SCOTT FISHER,
THOMAS M. WHITTAKER, CHRISTOPHER PAUL

Sponsored by the Irregular Warfare Technical Support Directorate

NATIONAL DEFENSE RESEARCH INSTITUTE

For more information on this publication, visit **www.rand.org/t/TLA732-1**.

About RAND

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Limited Print and Electronic Distribution Rights

Handbook for Tactical Operations in the Information Environment: Online Appendixes

The following two appendixes accompany the *Handbook for Tactical Operations in the Information Environment*, available at www.rand.org/t/TLA732-1. With a quick-reference format and series of illustrative vignettes, the handbook facilitates problem-solving and highlights how early-career officers in tactical units can contribute to operations in the information environment (OIE). Supplementing the guidance in the handbook, Online Appendix A presents an overview of force development tasks for OIE and lists joint and service-specific tasks. Online Appendix B defines some key terms and explains how they are used to help improve communication between commanders and OIE practitioners.

ONLINE APPENDIX A

Force Development Tasks for OIE

This appendix presents joint- and service-level, NATO, and tactical (mission) task lists associated with OIE.[1] You might be surprised to see that these task lists include fairly comprehensive sets of OIE-related tasks. This implies that OIE-related challenges are not the result of a lack of service-approved tasks or tactical tasks but, rather, a lack of inclusion, attention, or understanding. The full task lists are unclassified (except where noted) and can be accessed on public or Common Access Card (CAC)–enabled joint sites; the information here was current as of 2020.

Types of Tasks

The U.S. military uses the term **task** in several different ways. At the top levels, tasks guide force design by ensuring that the services are able to fulfill joint requirements, articulated in the **Universal Joint Task List** (UJTL). Each service also has its own task list to guide force development in accordance with Title 10 and other responsibilities. **Task lists** serve as the menu from which unit leadership creates the **mission-essential task list** (METL), which dictates the development and execution of a unit training plan. Finally, **tactical (mission) tasks** facilitate clear communication and understanding in the orders process.

The UJTL is a comprehensive list of all tasks the joint force is expected to be capable of performing. From the UJTL, the services develop task lists for their respective roles and missions: Army Universal Task List (AUTL), Marine Corps Task List (MCTL), Navy Task List (NTL), and Air Force Task List (AFTL). NATO also maintains a task list that demonstrates a particularly good understanding of IE-related tasks.

The following are examples of OIE-related tasks. There are innumerable opinions on exactly what qualifies as an OIE-related task, so the lists reflect an analytical judgment call. At a minimum, they provide a starting point for building a METL and for practitioners to help their leadership (especially when attached) better understand the capabilities they offer and assign them appropriate tasks.

[1] Online Appendix B provides more detail on their objectives and effects, along with a breakdown of what are referred to as **tactical mission tasks** in the Army and **tactical tasks** in the Marine Corps.

Universal Joint Task List (UJTL)

The UJTL is organized into four levels of tasks: strategic national, strategic theater, operational, and tactical (TA). When conducting tactical OIE, the tactical tasks are the most applicable, but there are relevant tasks at higher levels as well. Below is a selection of OIE-related tactical-level tasks from the UJTL.

TA 3.5	Employ Space Capabilities
TA 5.2.1	Operate Department of Defense Information Network (DODIN) Extension
TA 5.10	Manage the Electromagnetic Spectrum
TA 5.10.1	Employ Electronic Warfare (EW)
TA 5.10.1.1	Employ Electronic Attack (EA)
TA 5.10.1.2	Employ Electronic Warfare Support (ES)
TA 5.10.1.3	Employ Electronic Protection (EP)
TA 5.10.2	Coordinate Employment of Electronic Warfare (EW)
TA 5.5	Conduct Cybersecurity
TA 5.6	Employ Information Operations (IO)
TA 5.6.3	Perform Tactical Deception (TAC-D)
TA 5.6.5.2	Execute Cyberspace Attack
TA 5.6.5.3	Execute Defensive Cyberspace Operations (DCO)
TA 5.6.6	Employ Military Support to Information Operations (MISO)
TA 5.9.3	Conduct Civil Information Management (CIM)
TA 5.9.4	Conduct Civil-Military Operations (CMO)
TA 6	Protect the Force
TA 6.8	Employ Defensive Countermeasures

Service Task Lists

Army Universal Task List (AUTL)

The AUTL is organized according to the six Army warfighting functions:

1. Movement and Maneuver
2. Intelligence
3. Fires
4. Sustainment
5. Conduct Mission Command
6. Protection.

The warfighting functions are complemented by a list of "Tactical Mission Tasks and Military Operations," number 7 on the list.

The first number of each Army task (ART) corresponds to the warfighting function. It is worth noting that OIE-related tasks span the intelligence, mission command, and protection warfighting functions. The Army has not followed the Joint Staff or the Marine Corps in adopting "information" as a seventh warfighting function, but that would offer a means of organizing and consolidating OIE-related tasks. For brevity, this list does not include OIE-related subtasks.

ART 2.2	Provide Support to Situational Understanding
ART 2.3	Conduct Information Collection
ART 2.4	Provide Intelligence Support to Targeting and Information-Related Capabilities
ART 5.3	Conduct Knowledge Management and Information Management
ART 5.6	Integrate Space Operations
ART 5.7	Conduct Public Affairs Operations
ART 5.9	Conduct Cyber Electromagnetic Activities
ART 5.11	Conduct Military Deception
ART 5.12	Synchronize Information-Related Capabilities
ART 5.13	Conduct Soldier and Leader Engagement
ART 5.14	Employ Military Information Support Operations
ART 5.15	Conduct Civil Affairs Operations
ART 6.3	Implement Physical Security Procedures
ART 6.4	Conduct Operational Area Security
ART 6.10	Implement Operations Security

Marine Corps Task List (MCTL)

The MCTL is similarly organized under the Marine Corps warfighting functions, called major tasks. Although the Marine Corps adopted "information" as its seventh warfighting function in 2019, the MCTL does not reflect this change; given the range of OIE-related tasks, it might not do so. All OIE-related Marine Corps Tasks (MCTs) are currently under MCT 5 ("Exercise Command and Control"). The list below includes some key OIE-related capability subtasks.

MCT 5.4	Conduct Information Operations (IO)
MCT 5.4.1.1	Conduct Deception Operations
MCT 5.4.1.2	Conduct Electronic Warfare (EW)

MCT 5.4.1.3	Conduct Military Information Support Operations (MISO)
MCT 5.4.2	Conduct Operations Security (OPSEC)
MCT 5.4.2.2	Conduct Information Assurance
MCT 5.4.2.4	Conduct Cyberspace Operations
MCT 5.4.3	Provide Operations in the Information Environment (OIE) Reachback Support
MCT 5.4.3.1	Conduct Operations Security (OPSEC) Surveys
MCT 5.6	Conduct Communication Strategy and Operations (CommStrat)
MCT 5.9	Plan and Direct Cyberspace Operations
MCT 5.9.1	Plan and Direct Department of Defense Information Network (DODIN) Operations
MCT 5.9.2	Conduct Offensive Cyberspace Operations (OCO)
MCT 5.9.3	Plan and Direct Offensive Cyberspace Operations (OCO)
MCT 5.9.4	Conduct Defensive Cyberspace Operations (DCO)
MCT 5.9.5	Plan and Direct Defensive Cyberspace Operations (DCO)
MCT 5.10	Plan and Coordinate Support to Space Operations
MCT 5.11	Plan and Coordinate Electronic Warfare (EW) Efforts
MCT 5.14	Conduct Operations in the Information Environment (OIE)
MCT 5.14.1	Establish Information Command Center (ICC)
MCT 5.14.2	Assure Enterprise Command and Control Systems and Critical Systems
MCT 5.14.3	Conduct Information Environment Battlespace Awareness
MCT 5.14.4	Attack or Exploit Networks, Systems, and Information
MCT 5.14.5	Inform Domestic and International Audiences
MCT 5.14.6	Influence Foreign Target Audiences
MCT 5.14.7	Deceive Adversary Target Audiences
MCT 5.14.8	Control Information Environment Capabilities, Resources, and Activities
MCT 5.14.9	Plan and Direct Operations in the Information Environment

Universal Naval Task List (UNTL)

The UNTL follows the same format as the AUTL and the MCTL and is organized by the six overarching naval tasks:

1. Deploy/Conduct Maneuver
2. Develop Intelligence
3. Employ Firepower
4. Perform Logistics and Combat Service Support
5. Exercise Command and Control
6. Protect the Force.

Like the ARTs, OIE-related Navy tactical tasks (NTAs) are spread across its major tasks.

NTA 1.5.9	Conduct Information Superiority Operations
NTA 3.2.9	Conduct Non-Lethal Engagement
NTA 3.2.10	Integrate Tactical Fires
NTA 3.2.11	Conduct Computer Network Attack
NTA 4.8	Conduct Civil Affairs in Area
NTA 4.8.7	Establish/Operate a Civil-Military Operations Center (CMOC)
NTA 4.8.10	Manage Civil Information
NTA 4.8.11	Provide Foreign Civil Administration
NTA 4.8.12	Identify the Civil Military Environment
NTA 4.8.13	Conduct Key Leader Engagement
NTA 4.8.14	Build Support for US Operations
NTA 5.5	Conduct Information Operations (IO)
NTA 5.5.3	Conduct Military Information Support Operations (MISO)
NTA 5.5.4	Conduct Electronic Warfare Support (ES)
NTA 5.5.5	Perform Information Assurance
NTA 5.5.5.1	Provide Computer Network Defense
NTA 5.5.5.2	Perform Electronic Protection
NTA 5.5.6	Perform Spectrum Management
NTA 5.5.6.1	Control Electromagnetic Interference (EMI)
NTA 5.5.6.2	Assess Electromagnetic Environmental Effects (E3)
NTA 5.6	Conduct Acoustic Warfare

NTA 5.8	Conduct Public Affairs
NTA 5.8.1	Provide Public Affairs Counsel
NTA 5.8.2	Develop Public Affairs Communication Strategies, Themes and Messages
NTA 5.8.3	Produce Public Affairs and Visual Information Products
NTA 5.8.4	Release Public Affairs Information and Imagery
NTA 5.8.5	Enable Media and Public Access
NTA 5.8.6	Conduct Public Affairs and Visual Information Assessment
NTA 5.8.7	Conduct Live Broadcasts of Public Affairs Events
NTA 6.1	Enhance Survivability
NTA 6.1.2	Conduct Perception Management
NTA 6.1.2.1	Employ Operations Security
NTA 6.1.2.2	Conduct Deception in Support of Tactical Operations
NTA 6.1.3	Conduct Counterdeception
NTA 6.1.4	Conduct Counterpropaganda Operations
NTA 6.1.5	Conduct Counter–Intelligence, Surveillance, and Reconnaissance (C-ISR)

Air Force Task List (AFTL)

The AFTL is now classified Secret and therefore is not included here.

NATO Task List (NTL)

The NTL gives particularly thoughtful consideration to OIE and is organized similarly to the UJTL. The following selection of tactical-level tasks provides some insight into how NATO views OIE and highlights opportunities for collaboration with allies and partners.

TT 4.8.0	Plan and Integrate Tactical Military Information Operations
TT 4.8.1	Employ Tactical Military Information Operations (Mil INFO)
TT 4.8.2	Plan and Coordinate Military Information Operations Action
TT 4.8.3	Conduct Military Information Operations (Mil INFO OPS)
TT 4.8.4	Analyse Military Information Campaigns (MICs) to Determine
TT 4.8.5	Employ Information Security (INFOSEC) Practices and Procedures

TT 4.8.6	Employ Concealment and Deception Techniques
TT 4.8.7	Plan and Conduct Tactical Deception
TT 4.8.8	Assess Effectiveness of Tactical Deception Plan
TT 4.8.9	Execute Deception Plans
TT 4.8.10	Conduct PSYOPS
TT 4.8.11	Conduct EW
TT 4.8.12	Conduct Media Operations & Press Relations
TT 4.9.0	Plan and Conduct Public Information Activities (*) G 6.3
TT 4.10.0	Conduct Civil-Military Co-operation (CIMIC) Activities
TT 4.10.1	Conduct CIMIC Liaison (*) G 7.2
TT 4.10.2	Establish and Operate a CIMIC Centre (*) G 7.4
TT 4.10.3	Establish Assessment Reports (*) G 7.5
TT 5.1.6	Produce Photographic, Video, and Print Media
TT 5.1.7	Monitor Tactical Situation
TT 5.1.8	Execute Communications Security (COMSEC)
TT 5.1.9	Coordinate Combat Camera Activities in Area of Operations
TT 5.1.10	Execute C4 Policies and Procedures for the Area of Operations
TT 5.1.11	Execute Information Assurance (IA) Procedures
TT 5.1.12	Implement Electromagnetic Spectrum Management, Policy, Plans, Programs, and Direction for the Area of Operations
TT 7.4.12	Employ Information Security (INFOSEC) for Tactical Forces

ONLINE APPENDIX B

Objectives, Effects, and Tactical Tasks for OIE

OIE planning often gets hung up on differences in terminology, practice, and doctrine. This appendix attempts to provide some clarity on key terms and their relationships, which should improve communication between commanders and OIE practitioners.

Objectives and Effects

The following terms are arguably the most important for communicating commander's intent and defining mission accomplishment. They are listed in order of significance.[2]

> **objective:** 1. The clearly defined, decisive, and attainable goal toward which an operation is directed. 2. The specific goal of the action taken which is essential to the commander's plan.
>
> **effect:** 1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom.
>
> **task:** A clearly defined action or activity specifically assigned to an individual or organization that must be done as it is imposed by an appropriate authority.

More simply, the **objective** is the end goal of the mission. It is accomplished by achieving certain **effects**, and effects are achieved through the execution of **tasks**. This is true in both the physical and information environments.

There is some debate about whether there should be information-specific objectives or effects. Is it important to break out and elevate objectives/effects achieved by nonlethal fires?[3] Or is everyone ultimately trying to accomplish the same objective anyway? Joint doctrine takes the latter position. To illustrate this point, the definition of **fires** in joint doctrine: "The use of weapon systems or other actions to create specific lethal or nonlethal effects on a target."[4]

---

[2] Definitions are from U.S. Department of Defense, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., December 2020.

[3] You might hear **nonkinetic** used, but nonlethal is the doctrinal term. For more on these questions, see Joint Staff, J7, Deployable Training Division, *Insights and Best Practices Paper: Integration of Lethal and Nonlethal Actions*, 3rd ed., May 2016, and JP 3-09, *Joint Fire Suppor*t, Washington, D.C., April 10, 2019.

[4] JP 3-09, 2019, p. GL-6.

These "other actions" account for a large proportion of what occurs in OIE—namely, information operations (or, in some cases, influence activities).

The takeaway is that separately planning for OIE could hinder integration or worse. Instead, think of OIE as a fires capability—another way of achieving effects and objectives—that requires assigning tactical (mission tasks).

Objective Examples

JP 3-13, *Information Operations*, uses the term **IO objectives** but does not define it or list examples. It does, however, define IO, specifying the following adversary-focused actions: influence, disrupt, corrupt, and usurp, all of which could serve as objectives or effects.[5]

The Army's ATP 3-13.1, *The Conduct of Information Operations*, also offers the helpful insight on objectives. The following excerpts capture high-level points; we strongly encourage you to visit the section "Information Operations Objectives" in Chapter 4 of the ATP for more detail and guidance.[6]

> 4.35. IO objectives express specific and obtainable outcomes or effects that commanders intend to achieve in and through the information environment. . . . IO objectives do not stand alone but support the commander's operational intent. Based on the definition of IO, objectives are framed to accomplish the following:
>
> - Attack enemy or adversary decision making and the capabilities or conditions that facilitate that decision making.
> - Preserve friendly decision making and the capabilities or conditions that facilitate it.
> - Otherwise shape the information environment to provide operational advantage to friendly forces, including freedom of maneuver in this environment.
>
> 4-39. No prescriptive format exists for an IO objective. One possible format [describes the intended] effect, target or target audience, action, and purpose.
>
> 4-40. IO objectives are written in terms of effects, because the desired effect focuses the activities (tasks) of IRCs. For IO, a proper effect falls into one of three categories. [They are effects against the enemy or adversary, effects to defend friendly forces, and effects to shape the IE, all of which are defined.]

Effects Examples

Table B.1 provides an example of from the Marine Corps of how doctrinally approved tactical tasks can be used specify effects that can be achieved through OIE. While not perfect, the list shows how you can communicate with non-IO planners and commanders in standard operational vernacular.

---

[5] At the time of this writing, JP 3-13 (last updated in 2014) was expected to be revised or replaced. See JP 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

[6] ATP 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

Table B.1
IO Effects and Definitions

IO Effect	Definition
Destroy	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	Break or interrupt the flow of information.
Degrade	Reduce the effectiveness or efficiency of an adversary's command and control (C2) or communications 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 an adversary's decisions and actions.
Deny	Prevent the adversary from accessing and using critical information, systems, and services.
Deceive	Cause a person to believe what is not true. Military deception seeks to mislead an adversary's decisionmakers by manipulating their perception of reality.
Exploit	Gain access to an adversary's C2 systems to collect information or to plant false or misleading information.
Influence	Cause others to behave in a manner favorable to US forces.
Isolate	Seal off both physically and psychologically an adversary from its sources of support, to deny an adversary freedom of movement, and prevent an adversary unit from having contact with other adversary forces.
Protect	Take action to guard against espionage or capture of sensitive equipment and information.
Respond	React quickly to an adversary's IO attack or intrusion.

SOURCE: The definitions are taken directly from MCWP 3-32, *Marine Air-Ground Task Force Information Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, April 1, 2018, p. 1-5.

NOTES: The above list is accepted in joint doctrine as it pertains to OIE. The terms may not align with Marine Corps practice for describing the effects of lethal fires. To avoid misunderstanding, always define your terms when applying them to OIE-related tasks.

Tactical (Mission) Tasks

See Online Appendix A for OIE-relevant task lists. Here, we provide more detail on Army and Marine Corps tactical (mission) tasks—that is "a specific activity performed by a unit while executing a form of tactical operation or form of maneuver."[7]

Army

In the Army, tactical mission tasks are categorized as actions by friendly forces or effects on enemy forces. Table B.2 lists some common terms to describe **what** a particular task involves. This list is not comprehensive, but it serves as a helpful start for developing a common vernacular.

[7] This definition comes from FM 3-90-1, *Offense and Defense*, Vol. 1, Washington, D.C.: Headquarters, U.S. Department of the Army, March 2013, p. B-1. Again, these are referred to as **tactical mission tasks** in the Army and **tactical tasks** in the Marine Corps.

Table B.2
Common Terms to Describe Army Tactical Mission Tasks

Type	Example Terms
Actions by friendly forces	Attack by dire, breach, bypass, clear, control, counterreconnaissance, disengagement, exfiltrate, follow and assume, follow and support, occupy, retain, secure, seize, support by fire
Effects on enemy forces	Block, canalize, contain, defeat, destroy, disrupt, fix, isolate, neutralize, suppress, turn

SOURCE: FM 3-90-1, 2013, p. B-1, Table B-1.

Marine Corps

Marine Corps tactical tasks are defined in Marine Corps Doctrinal Publication (MCDP) 1-0, *Marine Corps Operations*, last updated in 2019. In an earlier but still recent revision, the Marine Corps expanded its appendix on tactical tasks and grouped them according to whether they were enemy-oriented, terrain-oriented, friendly force–oriented, or population-oriented. Table B.3 shows these groupings. Refer to MCDP 1 for full descriptions of the tasks, many of which explicitly note that a given task is relevant to OIE. For example, the enemy-oriented task "attack by fire" involves direct or indirect fires "in the physical domains and/or through the information environment."[8]

Table B.3
Marine Corps Tactical Tasks and Definitions

Orientation	Tasks
Enemy	Ambush, attack by fire, block, breach*, bypass, canalize, contain*, corrupt, deceive, defeat, degrade, deny, destroy, disrupt, exploit, feint, fix, influence*, interdict, isolate, neutralize, penetrate, reconnoiter*, support by fire, suppress
Terrain	Breach*, clear, control*, cordon*, occupy*, reconnoiter*, retain, secure*, seize
Friendly	Cover, disengage, displace, exfiltrate, follow and assume, follow and support, guard, protect, screen
Population	Advise, assess the population, assist, build/restore infrastructure, contain*, control*, coordinate with civil authorities, cordon*, enable civil authorities, exclude, influence*, occupy*, reconnoiter*, secure*, train, transition to civil control

SOURCE: MCDP 1, 2019, p. C2, Table C-1.

* Tasks with multiple classifications and applications.

[8] MCDP 1, *Marine Corps Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, March 29, 2019, p. C-2.

References

Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, Washington, D.C.: Headquarters, U.S. Department of the Army, October 2018.

ATP—*See* Army Techniques Publication.

Field Manual 3-90-1, *Offense and Defense*, Vol. 1, Washington, D.C.: Headquarters, U.S. Department of the Army, March 2013.

FM—*See* Field Manual.

Joint Publication 3-09, *Joint Fire Support*, Washington, D.C.: U.S. Joint Chiefs of Staff, April 10, 2019.

Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014.

Joint Staff, J7, Deployable Training Division, *Insights and Best Practices Paper: Integration of Lethal and Nonlethal Actions*, 3rd ed., Washington, D.C., May 2016.

JP—*See* Joint Publication.

Marine Corps Doctrinal Publication 1, *Marine Corps Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, March 29, 2019.

Marine Corps Warfighting Publication 3-32, *Marine Air-Ground Task Force Information Operations*, Washington, D.C.: Headquarters, U.S. Marine Corps, April 1, 2018.

MCDP—*See* Marine Corps Doctrinal Publication.

MCWP—*See* Marine Corps Warfighting Publication.

U.S. Department of Defense, *DoD Dictionary of Military and Associated Terms*, Washington, D.C., December 2020.