CTS1

SMARTBOOK

FIRST EDITION

- The Terrorist Threat
- Hybrid & Future Threats
- Forms of Terrorism (Tactics & Techniques)
- Counterterrorism Operations
- Critical Infrastructure
- Protection Planning & Preparation
- Countering Weapons of Mass Destruction
- Consequence Management

Counterterrorism, WMD & HYBRID THREAT

Guide to Terrorism, Hybrid and Emerging Threats

The Lightning Press

Norman M Wade

thelightningpress.com

CTS1

SMARTBOOK

Counterterrorism, WMD & HYBRID THREAT

Guide to Terrorism, Hybrid and Emerging Threats

The Lightning Press

Norman M Wade

The Lightning Press

2227 Arrowhead Blvd.
Lakeland, FL 33813
24-hour Voicemail/Fax/Order: 1-800-997-8827
E-mail: SMARTbooks@TheLightningPress.com
www.TheLightningPress.com

(CTS1) The Counterterrorism, WMD & Hybrid Threat SMARTbook

Guide to Terrorism, Hybrid and Emerging Threats

** This is the second printing of CTS1 (Jul 2017), incorporating an updated DNI World Threat Assessment and additional materials from START/GTD. An asterisk marks changed pages.*

ISBN: 978-1-935886-43-3

Photo Credits. Cover photo: U.S. Army Rangers assigned to 2nd Battalion, 75th Ranger Regiment, clear a building during a live fire exercise on Fort Hunter Liggett, Calif., Jan 23, 2014. The live fire training ensures Rangers maintain proficiency on their tactical skills. (U.S. Army photo by Pfc. Rashene Mincy/ Released.) Rear cover images in order: World Trade Center attack (Dan Howell/Shutterstock.com), terrorist wanted in video (FBI.GOV), and explosive ordnance disposal specialist (DoD photo by Sgt. Melissa Parrish, U.S. Army/Released).

Printed and bound in the United States of America.

(CTS1) Notes to Reader

Guide to Terrorism, Hybrid and Emerging Threats

Terrorism has evolved as a preferred tactic for ideological extremists around the world, directly or indirectly affecting millions of people. Terrorists use many forms of unlawful violence or threats of violence to instill fear and coerce governments or societies to further a variety of political, social, criminal, economic, and religious ideologies.

A **hybrid threat** is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually-benefiting effects. They can operate conventionally and unconventionally, employing adaptive and asymmetric combinations of traditional, irregular, and criminal tactics and using traditional military capabilities in old and new ways.

Counterterrorism activities and operations are taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. The purpose of CT is to disrupt, isolate, and dismantle terrorist organizations and networks to render them incapable of striking the homeland, US facilities and personnel, or US interests abroad.

Weapons of mass destruction (WMD) are chemical, biological, radiological, or nuclear (CBRN) weapons or devices capable of a high order of destruction and/or causing mass casualties. The terrorist threat is amplified by the proliferation of WMD and their potential use by terrorists. The existence of these materials and the potential for use by actors of concern precipitates the need to plan, prepare for, and counter their use.

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy - the infrastructure. **Protection** is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.

Consequence management refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.

SMARTbooks - DIME is our DOMAIN!

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)! Recognized as a "whole of government" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive professional library designed with all levels of Service in mind.

SMARTbooks can be used as quick reference guides during actual operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training. Visit **www.TheLightningPress.com**!

(CTS1) References

The following primary references were used to compile *CTS1: The Counterterrorism, WMD & Hybrid Threat SMARTbook.* All references are open-source, public domain, available to the general public, and/or designated as "approved for public release; distribution is unlimited." *CTS1: The Counterterrorism, WMD & Hybrid Threat SMARTbook* does not contain classified or sensitive material restricted from public release.

Joint Publications (JPs)

JP 3-12(R)	Feb 2013	Cyberspace Operations (Redacted)
JP 3-26	Oct 2014	Counterterrorism
JP 3-26*	Nov 2009	Counterterrorism
JP 3-28	Jul 2014	Defense Support to Civil Authority
JP 3-40	Oct 2014	Countering Weapons of Mass Destruction
JP 3-41	Jun 2012	Chemical, Biological, Radiological, and Nuclear Consequence Management

Army Doctrine Publication (ADP), Army Doctrine Reference Publications (ADRPs), Army Techniques Publications (ATPs), and Training Circulars (TCs)

ADP/ADRP 3-37	Aug 2012	Protection
ATP 3-11.41	Jul 2015	Multi-Service TTPs for CBRN Consequence Management Operations
TC 7-100	Nov 2010	Hybrid Threat

Other Publications and Manuals

U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century, Aug 2007.

DCSINT Handbook No. 1.02, Critical Infrastructure, Aug 2006.

TRADOC Pamphlet 525-3-1, The U.S. Army Operating Concept: Win in a Complex World 2020-2040, Oct 2014.

NIPP 2013, National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, Dept of Homeland Security, 2013.

Additional Reference Sources

Combating Terrorism Center at West Point

Federal Bureau of Investigation

National Consortium for the Study of Terrorism and Responses to Terrorism (START). Global Terrorism Database [Data file]. Retrieved from http://www.start.umd.edu/gtd

National Counterterrorism Center (NCTC)

U.S. Department of State, Bureau of Counterterrorism

** Editor's Note: Chapter one on "The Terrorist Threat" from the 2009 edition of JP 3-26 was not carried forward or updated to the 2014 edition. Because the chapter contained valuable doctrinal reference material on the terrorist threat, it is referenced extensively in this book.*

(CTS1) Foreword

The terrorist attacks of September 11, 2001, fundamentally transformed the United States national security establishment. In the years following, the United States government renounced its Cold War posture and embraced an entirely new security stance. The landmark changes put terrorism on the mind of all Americans- from government officials, to new immigrants, business travelers, school children, and ordinary citizens.

One of the most significant security threats to the people of the United States comes from international terrorism. Recent events have shown, tragically, that the treat from terrorism is likely to be with us for some time. Terrorists seek to inflict mass casualties without warning and are often motivated through extremist ideologies.

The terrorist threat is always evolving; therefore, it is important that we, as counterterrorism students and practitioners, stay as prepared and informed as possible on how to meet this threat.

I am very pleased to work with The Lightning Press on this *Counterterrorism, WMD & Hybrid Threat SMARTbook*. This SMARTbook sets out a comprehensive approach towards understanding the nature of domestic and international terrorism, state-sponsored terrorism, and the behaviors and characteristics of terrorists. It then explains the nature of hybrid threats, counterterrorism strategies, and counterterrorism tactics. The fundamentals of command and control, risk management, cyber threats, weapons of mass destruction, protection planning, consequence management, and workplace violence are all outlined and discussed in detail.

In publishing this SMARTbook, we aim to provide a single resource for a basic understanding of contemporary terrorism. It is written for the audience of citizens, students, and counterterrorism practitioners -- military and civilian. This timely volume provides a clear framework for understanding today's complex security threats. More importantly, it gives students a firm baseline for continuing terrorism and counterterrorism studies, and it gives practitioners a reference for how the U.S. government has organized to meet the threat from terrorist activity.

We at Henley-Putnam University, and our colleagues at Lightning Press, hope that through this SMARTbook, we will have the opportunity to make a unique contribution to the field of terrorism and counterterrorism, as well as open up new dialogue on this multifaceted topic.

Diane L. Maye, Ph.D.
Dean, Terrorism and Counterterrorism Studies
Henley-Putnam University

(CTS1) Acknowledgements

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic)!

Recognized as a "whole of government" doctrinal reference standard by military, national security and government professionals around the world, SMARTbooks comprise a comprehensive professional library designed with all levels of Soldiers, Sailors, Airmen, Marines and Civilians in mind. Applying informational art to doctrinal science, SMARTbooks make reference as easy as 1-2-3!

Our new "National Power" series is a nested collection of supporting and related titles, but with a different focus and "Whole of Government" domain scope (D-I-M-E: Diplomatic,Informational, Military, Economic). Authored by established subject matter experts and industry thought leaders, National Power SMARTbooks are in-depth, single-topic, multi-volume specialty books across multiple reference categories, coupled with the same unique SMARTbook series approach to reference/technical writing and informational art.

The author and publisher would like to thank and acknowledge the following individuals who contributed subject matter expert and thought-leader research, review and materials to this book (listed in order of appearance):

Dr. Diane Maye
Dr. Troy Mitchell
Dr. Tamara A. Mouras
Paul Beach
Jay Martin
Dr. Thomas Hennefer

Norman M. Wade
Author/Publisher
The Lightning Press SMARTbooks

(CTS1) Table of Contents

Chap 1

The Terrorist Threat

Chap 2

Hybrid & Future Threats

Chap 3

Forms of Terrorism (Tactics & Techniques)

Chap 4

Counterterrorism

Chap 5

Critical Infrastructure

Chap 6

Protection Planning & Preparation

Chap 7

Countering Weapons of Mass Destruction

Chap 8

Consequence Management (CM)

Chap 1

I. Terrorism (Overview/Introduction)

Ref: JP 3-26, Counterterrorism (Nov '09), chap 2 and JP 3-26 (2014), chap. 1.

America is at war with extremists who advocate and use violence to gain control over others and threaten our way of life. Violent extremists find it useful to mischaracterize the war as a religious or cultural clash (e.g., between Islam and the West). These violent extremists see the United States and other western societies as primary obstacles to achieving their political ends. The greatest strength of our society is its freedom and openness. The extremist networks will continue to exploit the seams in open societies around the globe, and consequently, the United States and partner nations remain vulnerable to terrorist violence designed to undermine those relationships and cause some members to abandon the struggle.

(Dan Howell / Shutterstock.com)

Terrorists use many forms of unlawful violence or threats of violence to instill fear and coerce governments or societies to further a variety of political, social, criminal, economic, and religious ideologies. Terrorists threaten the national power, sovereignty, and interests of the United States and our allies. Terrorists organize and operate in a number of ways. Some operate within transnational networks, others operate as small independent groups, and others operate alone. The terrorist threat is amplified by the proliferation of weapons of mass destruction (WMD) and their potential use by terrorists. The United States strives to enlist the support of the international community, adapts alliances, and creates new partnerships to facilitate regional solutions that contain and defeat terrorists, their organizations, and networks.

I. What is Terrorism?

Terrorism has been described as both a tactic and strategy; a crime and a holy duty; a justified reaction to oppression and an inexcusable action. Definition may depend on whose point of view is being represented. Terrorism has often been an effective tactic for the weaker side in a conflict. As an asymmetric form of conflict, terrorism projects coercive power with many of the advantages of military force at a fraction of the cost to the terrorist. Terrorism is a means -- a method -- to an objective.

Defining Terrorism

Ref: U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), pp. 1-2 to 1-6 and FBI.GOV.

The U.S. Department of Defense (DOD) approved definition of terrorism is: "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

For the purposes of this SMARTbook, this will be the standard definition. However, this is one of many definitions. A sampling of definitions by the Federal Bureau of Investigation (FBI) and the Department of State (DOS) illustrate the different perspectives of categorizing and analyzing terrorism.

The FBI uses this: "Terrorism is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." The U.S. Department of State uses the definition contained in Title 22 U.S.C. Section 2656f(d). According to this section, "terrorism" means "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents."

The National Counterterrorism Center (NCTC) uses this Title 22 definition of terrorism also in its annual reports of terrorism incidents around the world. These definitions stress the respective institutional concerns of the organizations using them. The FBI concentrates on the unlawful aspect in keeping with its law enforcement mission.

The Department of State concerns itself with politically motivated actions by sub-national or clandestine actors as functions affect international relations and diplomacy. Terrorism is "…fundamentally political so the political significance of major events is vital to determining meaningful responses."

Related Definitions

Terrorist

An individual who uses violence, terror, and intimidation to achieve a result. (JP 1-02)

Antiterrorism (AT)

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (JP 1-02)

Combating Terrorism (CbT)

Actions, including antiterrorism and counterterrorism, taken to oppose terrorism throughout the entire threat spectrum. Also called CbT. (JP 1-02. Source: JP 3-26)

Counterterrorism (CT)

Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals. Also called CT. (Approved for incorporation into JP 1-02. Source: JP 3-26)

Transnational Threat

Any activity, individual, or group not tied to a particular country or region that operates across international boundaries and threatens United States national security or interests. (JP 1-02. Source: JP 3-26)

Outside the United States Government, there are greater variations in what features of terrorism are emphasized in definitions. One comment used often is, "One state's terrorist is another state's freedom fighter." There is clearly a wide array of definitions for terrorism. Despite this, several common elements may assist in defining terrorism: political, psychological, violent, dynamic, and deliberate. The United Nations produced this description in 1992; "An anxiety inspiring method of repeated violent action, employed by semi-clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets." The UN has no internationally-agreed definition of terrorism. Yet in September 2006, the United Nations and its Member States demonstrated signs of collective progress in agreement to a global strategy to counter terrorism.

Terrorism, like a theatrical play, can be viewed as a deliberate presentation to a large audience in order to gain attention, spotlight a particular message, and seek a response favorable to the actor. The purpose of such actions can have sinister impact on national, regional, and global populations. Global communications provide a stage for near instantaneous media exploitation. Anxiety can increase as random or deliberate acts of terror often target civilians as victims. Similar to a play, the objective of the experience is to affect the feelings and attitudes of the audience.

Definitions of Terrorism in the U.S. Code

https://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition (accessed Mar '16)

18 U.S.C. § 2331 defines "international terrorism" and "domestic terrorism" for purposes of Chapter 113B of the Code, entitled "Terrorism":

International Terrorism

"International terrorism" means activities with the following three characteristics:

- Involve violent acts or acts dangerous to human life that violate federal or state law;
- Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- Occur primarily outside the territorial jurisdiction of the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.*

** FISA defines "international terrorism" in a nearly identical way, replacing "primarily" outside the U.S. with "totally" outside the U.S. 50 U.S.C. § 1801(c).*

Domestic Terrorism

"Domestic terrorism" means activities with the following three characteristics:

- Involve acts dangerous to human life that violate federal or state law;
- Appear intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
- Occur primarily within the territorial jurisdiction of the U.S.

Federal Crime of Terrorism

18 U.S.C. § 2332b defines the term "federal crime of terrorism" as an offense that:

- Is calculated to influence or affect the conduct of government by intimidation or • coercion, or to retaliate against government conduct; and
- Is a violation of one of several listed statutes, including § 930(c) (relating to killing or attempted killing during an attack on a federal facility with a dangerous weapon); and § 1114 (relating to killing or attempted killing of officers and employees of the U.S.).

II. Nature of the Enemy

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-2 to II-3.

Terrorist groups, regardless of ideology, origin, location, or organizational structure have some common basic needs to survive and remain credible to their followers: funding, security, an ability to produce and distribute propaganda, a support infrastructure, an ability to recruit, and the means to conduct violent acts against selected targets.

(Combating Terrorism Center)

The principal enemy is a transnational movement, consisting of extremist organizations, networks, and individuals – and their state and non-state supporters – which uses terrorism for ideological ends. For example, the brand of terrorism used by Islamic terrorist groups has included the use of children and the mentally challenged as unknowing participants in suicide-bombing attacks against both fellow civilians and government personnel alike. Unlike traditional military adversaries, these transnational terrorists have shown no tendency to be deterred, adding significantly to the complexity of countering them. This enemy is often educated, absolutely dedicated, highly motivated, and shows little restraint. Terrorists find freedom of action within physical and virtual safe havens by exploiting modern technology, the population, the civil liberties of the societies they attack, and their extreme ideology. A common extremist ideology is what links some often disparate organizations into terrorist networks. Although they may have differing local goals or objectives, ideological extremism is the foundation of this movement's overall success. It is the key to motivation, recruitment, and direct and indirect support, and serves as the basis for justifying terrorist actions no matter how abhorrent.

Our secondary enemy is the other collective VEOs that interfere with our CT efforts and which may transition to overt sponsorship of or active participation in direct action against the United States, our PNs, and our interests.

There are a variety of state and non-state actors identified with terrorism that have been generally categorized as opportunists, extremists, and terrorists. Often, the three may be indistinguishable.

Opportunists

Opportunists are members of criminal organizations (e.g., narcoterrorists), weapon proliferators, or state sponsors, who undercut the rule of law and governmental legitimacy, contributing to an environment of corruption and violence. Opportunists take advantage of opportunities as they arise. They often allow the existence of terrorist safe havens and sanctuaries in various regions of the world or provide mutual support to satisfy other interests. The United States is just beginning to understand the collusive nature of this criminal-extremist nexus—a convergence of opportunists' and extremists' interests. A key danger of the association are terrorists/extremists seeking to obtain and use, or threaten to use, WMD, may find their efforts assisted by those opportunists who might not endorse the extremists' views or methods but who are merely seeking financial gain.

IV. What Defines a Terrorist/Terrorist Group?

The term terrorist refers to those who commit acts of terrorism. Goals and objectives of terrorists and terrorist organizations differ throughout the world and range from regional single-issue terrorists to the aims of transnational radicalism and terrorism.

Terrorism is primarily a psychological act that communicates through violence or the threat of violence.

Common motivational categories include separatism, ethnocentrism, nationalism, and revolution. Ideological categories can be framed by political, religious, or social purpose. Domestic or indigenous terrorists are "home-grown," that is, they can be native born or naturalized citizens of a nation. They operate normally within and against their own country of residence. International or transnational terrorists can be visualized as operating primarily between two nations and their geographic region. International groups may operate in multiple countries, but retain a regional geographic focus for their activities. Terrorism is becoming more violent as terrorist organizations realize the value of notoriety due to spectacular attacks and the mass media exploitation that results.

Terrorist Behaviors, Characteristics, & Motivations

Terrorism is a rationally selected tactic usually employed in the pursuit of ideological aims. However, some individuals or small violent organizations that employ terrorist means may not always be concerned with particular causes or an avowed ideology. These terrorists may be motivated purely by a desire to commit violent acts. From a psychological behavioral perspective, terrorism may fulfill a compelling need and this form of terrorism treats avowed ideology and political causes as after the fact justification. Another behavioral perspective is one based on rational choice. Terrorism is a tactic selected after rational consideration of the costs and benefits in order to achieve an objective.

Singular personality profiles of terrorists do not exist. In general, terrorists often feel alienated from society, have a perceived grievance, or regard themselves as victims of an injustice. An examination of characteristics of terrorists include aspects of status, education and intellect, age, gender, and appearance.

Motivation categories describe terrorist groups in terms of their goals or objectives. Some of common motivational categories are separatist, ethnocentric, nationalistic, and revolutionary. Goals and objectives of terrorist organizations differ throughout the world and range from regional single-issue terrorists to the aims of transnational radicalism and terrorism. As the most prominent democracy and significant economic, military, and political power in the world, the U.S. is a convenient and appealing target for extremists.

See pp. 1-11 to 1-18 for further discussion.

Terrorist Organizational Models

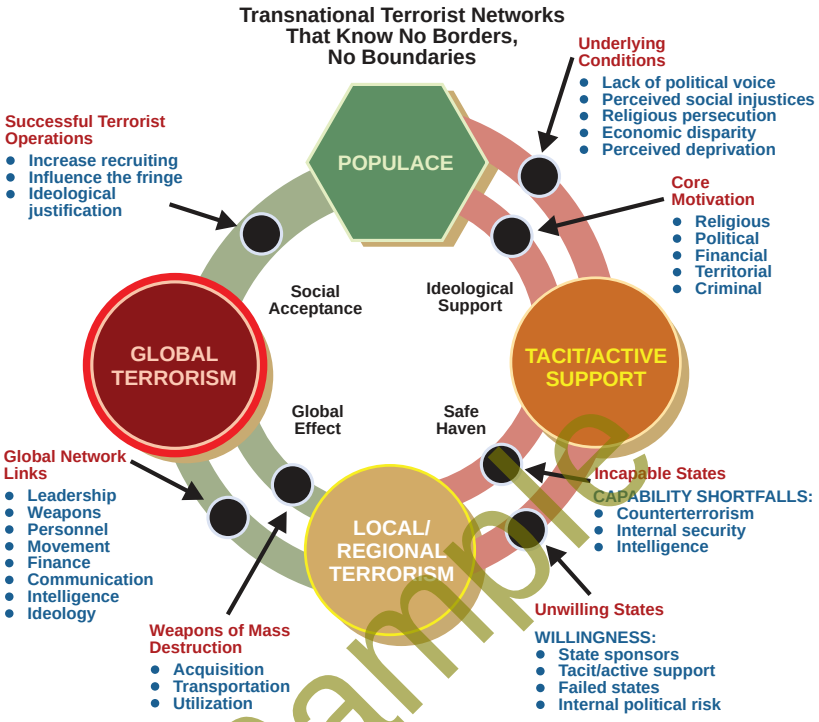
A terrorist organization's structure, membership, resources, and security determine its capabilities, influence, and reach. A general knowledge of the prevalent models of terrorist organizations helps to understand their overall capabilities. A terrorist organization is characterized by its levels of commitment, the tactical level cellular organization, group organizational structure, and its primary motivation.

Terrorists are now increasingly part of a far broader but indistinct system of networks than previously experienced. Groups based on religious or single-issue motives lack a specific political or nationalistic agenda and therefore have less need for a hierarchical structure to coordinate their actions. Instead, they can depend on loose affiliation with like-minded groups or individuals from a variety of locations. General goals and targets are announced, and individuals or cells are expected to use flexibility and initiative to conduct the necessary actions.

See pp. 1-19 to 1-24 for further discussion.

V. Terrorism Threat Model

Ref: JP 3-26, Counterterrorism (Nov '09), fig. III-2, p. III-8.



This representative model from JP 3-26 (2009) shows how violent extremist organizations (VEOs) can use terrorism as a circle that operates around four critical components:

- **A populace** from which extremists have the potential to draw support
- **Tacit and/or active support** given to the extremist by some of the sympathetic populace
- **Local/regional terrorism** as a result of states unwilling or incapable of countering violent extremists
- **Global terrorism** that results from global networks built upon popular support and the inability of states to control local and regional extremist networks

The cycle is completed when successful terrorist operations (at the global or local/regional level) reinforce their ideological justification, and influence that portion of the populace that is susceptible to the extremist ideology.

VII. Forms of Terrorism

Terrorism is one of the oldest forms of human conflict. Before societies organized to wage war against each other, individuals and small bands engaged in terror tactics to achieve limited goals–to overthrow existing leaders, toward off potential rivals, or to frighten opposing groups from lands they wished to claim for themselves.

Forms of terrorism threats range non-state transnational networks with global reach capability such as al-Qaida, terrorist cells affiliated with regional or international aims, or individual self-radicalized and unaffiliated terrorists with single issue agendas. Yet, each type of network or terrorist cell has criminal intentions limited by finite capability. Terrorists exist as a foreign and domestic threat of the United States in the U.S. Homeland and in United States presence throughout the world.

Although the means and ends have evolved throughout history, the central elements of terrorism–fear, panic, violence, and disruption–have changed little through time. As the world enters the 21st Century, terrorism remains a vexing problem–an anachronistic fixture of human relations as paradoxically human and inhuman in the third Millennium as it was before the dawn of recorded history.

See chap. 3, "Forms of Terrorism", for further discussion.

A. State-Sponsored Terrorism

Some nations and states often resort to violence to influence segments of their population, or rely on coercive aspects of state institutions. National governments can become involved in terrorism or utilize terror to accomplish the objectives of governments or individual rulers. Most often, terrorism is equated with non-state actors or groups that are not responsible to a sovereign government. However, internal security forces can use terror to aid in repressing dissent, and intelligence or military organizations can perform acts of terror designed to further a state's policy or diplomatic efforts abroad.

See pp. 1-25 to 1-30 for further discussion.

B. International Terrorism

International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

See pp. 1-31 to 1-74 for further discussion.

C. Domestic Terrorism

Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

See pp. 1-75 to 1-84 for further discussion.

II. Terrorist Behavior, Characteristics, Motivations

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-4 to II-8, and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), chap. 2.

The following discussion provides an insight into terrorist behaviors at both the individual and group levels, examines the impact of group goals and motivations on terrorist planning and operations, and provides observations of general terrorist characteristics. Goals and objectives of terrorist organizations differ throughout the world and range from regional single-issue terrorists to the aims of transnational radicalism and terrorism.

(FBI.GOV)

Terrorism is primarily a psychological act that communicates through violence or the threat of violence. Common motivational categories include separatism, ethnocentrism, nationalism, and revolution. Ideological categories can be framed by political, religious, or social purpose.

Domestic or indigenous terrorists are "home-grown," that is, they can be native born or naturalized citizens of a nation. They operate normally within and against their own country of residence. International or transnational terrorists can be visualized as operating primarily between two nations and their geographic region. International groups may operate in multiple countries, but retain a regional geographic focus for their activities. Terrorism is becoming more violent as terrorist organizations realize the value of notoriety due to spectacular attacks and the mass media exploitation that results.

I. Terrorist Behavior

Terrorism is a rationally selected tactic usually employed in the pursuit of ideological aims. However, some individuals or small violent organizations that employ terrorist means may not always be concerned with particular causes or an avowed ideology. These terrorists may be motivated purely by a desire to commit violent acts. From a psychological behavioral perspective, terrorism may fulfill a compelling need and this form of terrorism treats avowed ideology and political causes as after the fact justification. Another behavioral perspective is one based on rational choice. Terrorism is a tactic selected after rational consideration of the costs and benefits in order to achieve an objective.

A. Individual Terrorist Behaviors

Utopian View

Some terrorists have utopian goals regardless of their aims. This utopianism expresses itself forcefully as an extreme degree of impatience with the "status quo" of the rest of the world that validates the terrorists' extreme methods. This view commonly perceives a crisis too urgent to be solved other than by the most extreme methods. Alternately, the perception is of a system too corrupt or ineffective to see or adopt the "solution" the terrorist espouses. This sense of desperate impatience with opposition is central to the terrorist world view. This is true of both the secular and religiously motivated terrorist, although with slightly different perspectives as to how to impose their solutions. There is also a significant impractical element associated with this utopian mind-set. Although their goals often involve the transformation of society or a significant reordering of the status quo, individual terrorists, even philosophical or intellectual leaders, are often vague or uncaring as to what the future order of things will look like or how their ideas will be implemented. Change, and the destructive method by which change is brought about, may be much more important than the end result.

Interaction with Others

Terrorists interact within their groups at both the member and leadership levels. Individuals forming or joining groups normally adopt the "leader principle" which amounts to unquestioning submission to the group's authority figure. This explains the prevalence of individual leaders with great charisma in many terrorist organizations. Such leaders can demand tremendous sacrifices from subordinates. This type of obedience can cause internal dissension when a leader is at odds with the group or factions arise in the organization. Another adaptation of the individual is accepting an "in-group" (us against the world) mentality. This results in a presumption of automatic morality on the part of the other members of the group, and purity of their cause and goals. Thus, violence is necessary and morally justified and the use of violence becomes a defining characteristic.

Dehumanization of Nonmembers

There is a dehumanization of all "out-group" individuals. This dehumanization permits violence to be directed indiscriminately at any target outside the group. Dehumanization also removes some of the stigma regarding the killing of innocents. Another aspect is that by making the oppressed people an abstract concept, it permits the individual terrorist to claim to act on their behalf.

Lifestyle Attractions

A terrorist may choose violence as a lifestyle. It can provide emotional, physical, perceived religious, and sometimes social rewards. Emotionally, the intense sense of belonging generated by membership in an illegal group can be satisfying. Physical rewards can include such things as money, authority, and adventure. This lure often can subvert other motives. Social rewards may be a perceived increase in social status or power.

Impact of Terrorist Goals and Motivations on Planning

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-6 to II-7.

Strategies against terrorists require understanding their point of view. Understanding and knowledge of VEO's preferences and capabilities provides a baseline to conduct successful CT operations and promotes the use of active approaches, both direct and indirect, to counter the threat.

Terrorist Asset Cost Versus Target Value

Terrorist groups require recruitment, preparation, and integration into the operational structure of the group. Recruits also require extensive vetting to ensure that they are not infiltrators. A group's leadership will not employ assets without weighing the value of the asset, the probability of success, and the potential benefits to the group. For example, suicide bombings are on the increase. This type of terrorist attack provides effective target results for relatively low cost. Normally in a terrorist operation, extensive preoperational surveillance and reconnaissance, exhaustive planning, and sufficient resources will be committed to the operation.

Operational Intent of Terrorism

At the fundamental level, terrorism is a psychological act that communicates through the medium of violence or the threat of violence. Terrorist strategies are aimed at publicly causing damage to symbols or inspiring fear. Timing, location, and method of attacks accommodate media dissemination and ensure wide-spread reporting to maximize impact. In its purest form, a terrorist operation often will have the goal of manipulating popular perceptions, and strives to achieve this by controlling or dictating media coverage. This control need not be overt, as terrorists analyze and exploit the dynamics of major media outlets and the pressure of the "news cycle." In considering possible terrorist targets, a massive destructive attack launched against a target that does not attract media coverage may not be a suitable target for the intended effect and targeted population.

Ideological and Motivational Influences on Operations

Ideology and motivation are the primary characteristics that influence the objectives of terrorist operations. Groups with secular ideologies and nonreligious goals often will attempt highly selective and discriminate acts of violence to achieve a specific political aim. This often requires the terrorist group to keep casualties to the minimum amount necessary to attain the objective. This is both to avoid a backlash that might severely damage the organization and to also maintain the appearance of a rational group that has legitimate grievances. By limiting their attacks, the group reduces the risk of undermining external political and economic support. Groups that comprise a "wing" of an insurgency, or are affiliated with sometimes legitimate political organizations often operate under these constraints. The tensions caused by balancing these considerations are often a prime factor in the development of splinter groups and internal factions within these organizations. In contrast, religiously oriented groups typically attempt to inflict as many casualties as possible. An apocalyptic frame of reference may deem loss of life as irrelevant and encourage mass casualty producing incidents. Losses among this group are of little account because such casualties will reap the benefits of the afterlife. Likewise, nonbelievers, whether they are the intended target or collateral damage, deserve death, because their killing may be considered a moral duty. Another common form of symbolism in terrorist targeting is striking on particular anniversaries or commemorative dates.

Motivations of Terrorist Organizations: Goals & Objectives (Cont.)

Continued from previous page

Religious motivations can also be tied to ethnic and nationalist identities, such as Kashmiri separatists who combine their desire to break away from India with the religious conflict between Islam and Hinduism. Numerous religious denominations have either seen activists commit terrorism in their name, or spawned cults professing adherence to the larger religion while following unique interpretations of that particular religion's dogma. Cults that adopt terrorism are often apocalyptic in their worldview, and are extremely dangerous and unpredictable. Of note, religiously inspired cults executed the first confirmed uses of biological and chemical nerve agents by terrorists.

Social

Often particular social policies or issues will be so contentious that they will incite extremist behavior and terrorism. Frequently this is referred to as "single issue" or "special interest" terrorism.

D. Location or Geographic Categories

Geographic designations have been used in the past, and although they are often confusing, and even irrelevant when referring to international and transnational terrorism, they still appear. Often, a geographical association to the area with which the group is primarily concerned will be made. "Mid-Eastern" is an example of this category and came into use as a popular shorthand label for Palestinian and Arab groups in the 1970s and early 1980s. Frequently, these designations are only relevant to the government or state that uses them. However, when tied to particular regions or states, the concepts of domestic and international terrorism can be useful.

Domestic or Indigenous

These terrorists are "home-grown" and operate within and against their home country. They are frequently tied to extreme social or political factions within a particular society, and focus their efforts specifically on their nation's sociopolitical arena.

International

Often describing the support and operational reach of a group, "international" and "transnational" are often loosely defined. International groups typically operate in multiple countries, but retain a geographic focus for their activities. For example, Hezbollah has cells worldwide, and has conducted operations in multiple countries, but is primarily focused on influencing the outcome of events in Lebanon and Israel. An insurgency-linked terrorist group that routinely crosses an international border to conduct attacks, and then flees to safe haven in a neighboring country, is "international" in the strict sense of the word, but does not compare to groups that habitually operate across regions and continents.

Transnational

Transnational groups operate internationally, but are not tied to a particular country, or even region. Al-Qaeda is transnational; being made up of many nationalities, having been based out of multiple countries simultaneously, and conducting operations throughout the world. Their objectives affect dozens of countries with differing political systems, religions, ethnic compositions, and national interests.

Continued from previous page

Terrorist Levels of Commitment

Ref: JP 3-26, Counterterrorism (Nov '09), chap. 2, pp. 2-8 to 2-10 (fig. 2-1, p. 2-9).

Typically, there are four different levels of commitment within a terrorist organization: passive supporters, active supporters, cadre, and leadership.

Leaders

Leaders provide direction and policy; approve goals and objectives; and provide overarching guidance for operations. Usually leaders rise from within the ranks of any given organization, or create their own organization, and are ruthless, driven, and very operationally oriented in order to accomplish their objectives.

Cadre

Cadre is the nucleus of "active" members, the zealots, who comprise the core of a terrorist organization. This echelon plans and conducts not only operations, but also manages areas of intelligence, finance, logistics, IO, and communications. Mid-level cadres tend to be trainers and technicians such as bomb makers, financiers, and surveillance experts. Low-level cadres are the bombers and foot soldiers for other types of attacks.

Active Supporters

Active supporters participate in the political, fund-raising, and information activities of the group. Acting as an ally or tacit partner, they may also conduct initial intelligence and surveillance activities, and provide safe houses, financial contributions, medical assistance, and transportation assistance for cadre members. Usually, they are fully aware of their relationship to the terrorist group but do not commit violent acts.

Passive Supporters

Passive supporters are typically individuals or groups that are sympathetic to the announced goals and intentions of the terrorist organization or its ideology, but are not committed enough to take action. Passive supporters may interact with a front group that hides the overt connection to the terrorist group, or passive supporters may intermingle with active supporters without being aware of what their actual relationship is to the organization. Sometimes fear of reprisal from terrorists compels passive support. Sympathizers can be useful for political activities, fund-raising, and unwitting or coerced assistance in intelligence gathering or other nonviolent activities.

IV(a). State-Sponsored Terrorism

Ref: U.S. Department of State; and the National Counterterrorism Center (NCTC); and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), pp. 1-9 to 1-11.

Some nations and states often resort to violence to influence segments of their population, or rely on coercive aspects of state institutions. National governments can become involved in terrorism or utilize terror to accomplish the objectives of governments or individual rulers. Most often, terrorism is equated with non-state actors or groups that are not responsible to a sovereign government. However, internal security forces can use terror to aid in repressing dissent, and intelligence or military organizations can perform acts of terror designed to further a state's policy or diplomatic efforts abroad.

Ref: U.S. Department of State, Bureau of Counterterrorism.

Countries determined by the Secretary of State to have repeatedly provided support for acts of international terrorism are designated pursuant to three laws: section 6(j) of the Export Administration Act, section 40 of the Arms Export Control Act, and section 620A of the Foreign Assistance Act. Taken together, the four main categories of sanctions resulting from designation under these authorities include restrictions on US foreign assistance; a ban on defense exports and sales; certain controls over exports of dual use items; and miscellaneous financial and other restrictions.

Designation under the above-referenced authorities also implicates other sanctions laws that penalize persons and countries engaging in certain trade with state sponsors.

To designate a country as a State Sponsor of Terrorism, the Secretary of State must determine that the government of such country has repeatedly provided support for acts of international terrorism. Once a country is designated, it remains a State Sponsor of Terrorism until the designation is rescinded in accordance with statutory criteria.

A wide range of sanctions are imposed as a result of a State Sponsor of Terrorism designation, including:

- A ban on arms-related exports and sales
- Controls over exports of dual-use items, requiring 30-day Congressional notification for goods or services that could significantly enhance the terrorist-list country's military capability or ability to support terrorism
- Prohibitions on economic assistance
- Imposition of miscellaneous financial and other restrictions

B. Sudan

http://www.state.gov/j/ct/rls/crt/2014/239410.htm (Accessed Mar 2016)

Sudan was designated as a State Sponsor of Terrorism in 1993 due to concerns about support to international terrorist groups. Sudan remained a generally cooperative partner of the United States on counterterrorism. During the past year, the Government of Sudan continued to support counterterrorism operations to counter threats to U.S. interests and personnel in Sudan.

Elements of al-Qa'ida-inspired terrorist groups remained in Sudan. The Government of Sudan has taken steps to limit the activities of these elements and has worked to disrupt foreign fighters' use of Sudan as a logistics base and transit point for terrorists going to Syria and Iraq. However, groups continued to operate in Sudan in 2014 and there continued to be reports of Sudanese nationals participating in terrorist organizations.

In 2014, Sudan continued to allow members of Hamas to travel, fundraise, and live in Sudan.

In June 2010, four Sudanese men sentenced to death for the January 1, 2008 killing of two U.S. Embassy staff members escaped from Khartoum's maximum security Kober prison. That same month Sudanese authorities confirmed that they recaptured one of the four convicts and a second escapee was reported killed in Somalia in May 2011. The recaptured murderer is being held in Kober Prison, and as of December 2014, appeals of his pending death sentence were still ongoing. The whereabouts of the other two convicts are unknown.

In February 2013, one of five men convicted of aiding the 2010 escape attempt by the four convicted killers received a presidential commutation of his remaining sentence. Sudanese authorities explained his release was part of a broad administrative parole affecting 200 other prisoners who had served some portion of their sentences with good behavior. U.S. government officials protested the commutation and urged Sudanese authorities to imprison the convicted accomplice for the full 12 years of his sentence. The individual remained free on parole at year's end.

Sudanese authorities this year released most of the 25 individuals detained in a December 2012 raid on what the Government of Sudan described as a terrorist training camp operating in Dinder National Park. Members of the so-called "Dinder cell" were charged with terrorism and murder stemming from the deaths of several police involved in the December 2012 raid. One trial judge from the country's terrorism court remanded several cases back to the attorney general for additional interrogations and those accused continued to be held in prison. The remaining Dinder detainees have had sessions with Dr. Essam Ahmed al-Basher, who helps lead the Government of Sudan's "extremist rehabilitation program."

In general, the Government of Sudan appeared to oppose the financing of extremist elements. Sudanese officials have welcomed Hamas members to Khartoum, however, and its members are permitted to conduct fundraising in Sudan. The Central Bank of Sudan and its financial intelligence unit, renamed the Financial Information Unit in late 2014, circulated to financial institutions a list of individuals and entities that have been included on the UN 1267 sanctions committee's consolidated list, as well as the U.S. government's lists of terrorist organizations/financiers. The financing of terrorism per UN Resolution 1373 was criminalized in Sudan pursuant to Sudan's Money Laundering Act of 2003.

Additionally, Sudan has yet to take concrete steps to resolve the crisis in the Two Areas of Southern Kordofan and Blue Nile, to include ending aerial bombardments, allowing sufficient and sustained humanitarian access, and resuming political dialogue to resolve the conflicts.

IV(b). International Terrorism

Ref: U.S. Department of State, Bureau of Counterterrorism; and the National Counterterrorism Center (NCTC).

A number of resources available to assess the current terrorist threat. The following sections are provided as an overview to several of these resources.

I. Country Reports on Terrorism and Patterns of Global Terrorism

Ref: http://www.state.gov/j/ct/rls/crt/132196.htm

U.S. law requires the Secretary of State to provide Congress, by April 30 of each year, a full and complete report on terrorism with regard to those countries and groups meeting criteria set forth in the legislation. This annual report is entitled Country Reports on Terrorism. Beginning with the report for 2004, it replaced the previously published Patterns of Global Terrorism.

The report covers developments in countries in which acts of terrorism occurred, countries that are state sponsors of terrorism, and countries determined by the Secretary to be of particular interest in the global war on terror. As provided in the legislation, the report reviews major developments in bilateral and multilateral counterterrorism cooperation as well.

The report also provides information on terrorist groups responsible for the death, kidnapping, or injury of Americans, any umbrella groups to which they might belong, groups financed by state sponsors of terrorism, reports on all terrorist organizations on the Foreign Terrorist Organization (FTO) list, and other terrorist groups determined by the Secretary to be relevant to the report.

Beginning with the report for 2005, Country Reports on Terrorism will also address terrorist sanctuaries and terrorist attempts to acquire weapons of mass destruction. It will also include statistical information provided by the National Counterterrorism Center (NCTC) on the number of individuals killed, injured, or kidnapped by terrorist groups.

Replacing Patterns of Global Terrorism with Country Reports on Terrorism

Since September 11, 2001, changes in organization and responsibilities in the intelligence community, combined with the dynamic pace of the global war on terrorism, prompted the Department of State to take a fresh look at Patterns of Global Terrorism, its contents and its governing legislation.

In July 2004, the 9/11 Commission recommended creation of a National Counterterrorism Center (NCTC) to provide an authoritative agency for all-source analysis of global terrorism. The President implemented the recommendation by executive order in August 2004, and the agency was created via the Intelligence Reform and Terrorism Prevention Act the following December.

That law designates the NCTC as the primary organization for analysis and integration of "all intelligence possessed or acquired by the United States government pertaining to terrorism or counterterrorism." It further states that the NCTC would be the government's "shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contact and support."

V. Combating Terrorism Center at West Point

https://www.ctc.usma.edu/

The Combating Terrorism Center is an independent, privately funded, research and educational institution situated at West Point that contributes to the academic body of knowledge and informs counterterrorism policy and strategy.

Mission

Situated at the nexus of theory and practice, the Combating Terrorism Center serves as an important national resource that rigorously studies the terrorist threat and provides policy-relevant research while moving the boundaries of academic knowledge. The CTC's distinguished scholars, international network of experts, and access to senior U.S. government leadership set it apart from any other like enterprise.

A. Counterterrorism Practitioner Education

The Combating Terrorism Center is the largest provider of counterterrorism and countering violent extremism (CVE) education to federal, state, and local government in the United States. From assisting FDNY leadership with an 11 week graduate seminar, to educating every new special agent at the FBI, to providing seminars to the Intelligence Community; the Combating Terrorism Center remains committed to an educational model that promotes interagency, multi-jurisdictional educational events. Since defeating terrorist threats depends on a unity of effort, it is imperative that our programs not only provide relevant information but also strengthen professional networks and collaboration between multiple stakeholders. Partner institutions include:

- FBI-CTC Collaboration
- FDNY Counterterrorism Leadership Program
- Department Of Justice Education
- Department Of Homeland Security Education

B. Research Philosophy & Publications

The Combating Terrorism Center is one of the leading academic institutions devoted to the study of terrorism. The four topical programs outlined below comprise the core of our research agenda, and reflect our understanding of the key contemporary terrorism issues sets facing academics and government officials.

Research areas and sample featured publications include:

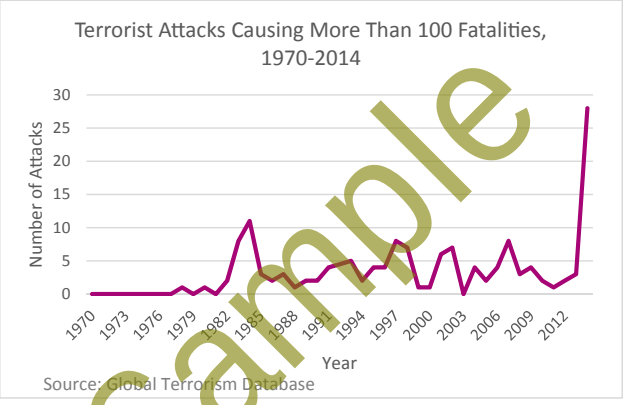
Continued from previous page

Overview: Terrorism in 2014 (Cont.)

Casualties

Several new trends emerged with respect to casualties of terrorist attacks in 2014. In particular, the proportion of total fatalities that were perpetrator fatalities (24%) is the highest recorded since collection of the GTD began in 1970. Perpetrator fatalities are a result of several different scenarios: suicide attacks in which the perpetrators intend to kill themselves; accidental deaths of perpetrators killed while attempting to carry out an attack; or attacks, targeting either combatants or non-combatants, in which security forces respond and a clash ensues.

In 2014, 39 percent of the attacks in which perpetrators were killed were suicide attacks, compared to 51 percent in 2013 and 42 percent in 2012. Of the remaining attacks, 45 percent targeted the military, and 30 percent targeted police. Among countries that experienced at least 50 fatalities from terrorist attacks in 2014, those with the highest proportion of perpetrator fatalities were Uganda (77% of 98 fatalities), Cameroon (73% of 788 fatalities), China (50% of 322 fatalities), and Afghanistan (46% of 5,411 fatalities).



A second trend regarding casualties in 2014 pertains to the frequency of extreme mass-fatality terrorist attacks. Worldwide, the number of attacks involving more than 100 fatalities increased to 28, from three in 2013. These attacks took place in Nigeria (9 attacks), Iraq (7), Syria (4), Cameroon (3), Ukraine (2), South Sudan (1), Sudan (1), and Pakistan (1). The most common perpetrator organizations were Boko Haram (11 attacks) and the Islamic State of Iraq and the Levant (ISIL; 11). Combined, these 28 attacks caused more than 7,300 fatalities (17% of all fatalities worldwide throughout 2014), including more than 2,000 perpetrator fatalities (20% of all perpetrator fatalities worldwide throughout 2014).

Several attacks in 2014 were the deadliest attacks in recent history. For example, in June, ISIL claimed responsibility for an attack in which assailants seized a prison in Badush, Iraq, and killed 670 Shi'a prisoners, while freeing Sunni prisoners. Also in June, members of ISIL abducted and killed at least 1,500 Iraqi soldiers at Camp Speicher in Tikrit, Iraq. In August, ISIL assailants attacked Yazidi civilians in Sinjar, Iraq, killing at least 500 and abducting 300 others, many of whom were ultimately released in 2015.

Perpetrators

ISIL and the Taliban were responsible for the most terrorist attacks in 2014, with 28 percent of all attacks for which a perpetrator organization was identified. These organizations, along with Boko Haram, were also responsible for an increasingly disproportionate number of fatalities—59 percent of all fatalities caused by attacks in which a perpetrator organization was identified, compared to 46 percent in 2013.

Continued from previous page

VIII. Terrorist Group Profiles

Representative profiles of terrorist groups from the NCTC and the Department of State's Foreign Terrorist Organization list are provided on the following pages:

Under US law, NCTC focuses exclusively on international terrorism. There are other organized groups that engage in violent acts—some are criminal organizations with no political or social agenda, and some are domestic terrorist groups; however, this guide reflects NCTC's international focus. Senior Intelligence Community officials assess the greatest international terrorist threats currently facing the United States come from violent extremists inspired by al-Qa'ida, including its allies and affiliates, who are committed to conducting attacks inside the United States and abroad.

Islamic State of Iraq and the Levant (ISIL)

Abu Bakr al-Baghdadi

The Islamic State of Iraq and the Levant (ISIL)—formerly known as al-Qa'ida in Iraq and Islamic State of Iraq—was established in April 2004 by long-time Sunni extremist Abu Mus'ab al-Zarqawi, who the same year pledged his group's allegiance to Usama Bin Ladin. ISIL targeted Coalition forces and civilians using high-profile tactics such as vehicle-borne improvised explosive devices (VBIEDs), suicide bombers, and hostage executions, to pressure foreign countries and companies to leave Iraq, push Iraqis to stop supporting the United States and the Iraqi Government, and attract additional cadre to its ranks.

Following al-Zarqawi's death in June 2006, ISIL's new leader, Abu Ayyub al-Masri, announced in October 2006 the formation of the Islamic State of Iraq, led by Iraqi national Abu 'Umar al-Baghdadi, in an attempt to politicize the group's terrorist activities and place an "Iraqi face" on their efforts.

In 2007, ISIL's continued targeting and repression of Sunni civilians in Iraq caused a widespread backlash—known as the Sunni Awakening—against the group. The development of the Awakening Councils—composed primarily of Sunni tribal and local community leaders—coincided with a surge in Coalition and Iraqi Government operations, resulting in a decreased attack tempo beginning in mid-2007.

ISIL's current leader, Abu Bakr al-Baghdadi, assumed power following the death of both Abu Ayyub al-Masri and Abu 'Umar al-Baghdadi in April 2010. Under his authority, the group has continued conducting high-profile attacks across Iraq. ISIL has expanded its ranks through prison breaks and integration of fighters drawn to the Syrian conflict.

In April 2013, Abu Bakr al-Baghdadi publicly declared the group's presence in Syria under the name ISIL and that ISIL had founded the al-Nusrah Front in Syria. Al-Nusrah Front in June 2013 publicly pledged allegiance to al-Qa'ida leader Ayman al-Zawahiri. The disagreement and ISIL's hardline ideology caused a backlash in Syria. ISIL rejected al-Nusrah Front, Syrian opposition enemies, and al-Qa'ida's efforts to force the group to leave Syria.

In February 2014, al-Qa'ida publicly stated ISIL was no longer a branch of al-Qa'ida, a status the group had held since 2004. ISIL in April 2014 responded to the disavowal by publicly attacking al-Qa'ida as being unfit for Usama Bin Ladin's legacy and stating that ISIL was a better example for jihadists. Major ISIL-led efforts to overthrow the Iraqi Government erupted in June 2014, freeing prisoners and gaining access to more weapons and vehicles usable in Iraq or Syria. In late June 2014, ISIL declared the establishment of an Islamic caliphate under the name the "Islamic State" and called for all Muslims to pledge allegiance to the group.

IV(c). Domestic Terrorism

Contributor: Dr. Troy Mitchell.

Since September 11, 2001, the terrorist attacks and the U.S. response—now called the global war on terrorism—have changed the world, and the terrorist enterprise that we know as al-Qaeda has morphed into a globalized enterprise. As the most destructive day in the long, bloody history of terrorism, the casualties, economic damage, and outrage were unprecedented. The current status of al-Qaeda's network remains unclear, but it is certain that it and other terrorist groups continue to threaten the lives and well-being of civilians, at home and abroad, and the security of our friends and allies. This continuing danger leads to ongoing U.S. and international efforts to monitor, disrupt, and dismantle terrorist groups before they cause large-scale destruction to our people or our interests. The tremendous number and variation of terrorist organizations in the world preclude a single causal explanation for terrorism relative to every situation. Terrorist organizations appeal disproportionately to certain psychological types of people, namely, the socially alienated.

(AP Photo/Charles Krupa)

In this April 15, 2013 photo, an emergency responder and volunteers, including Carlos Arredondo in the cowboy hat, push Jeff Bauman in a wheel chair after he was injured in an explosion near the finish line of the Boston Marathon in Boston. The twin bombing at the Boston Marathon killed three people and wounded more than 260 others. Prosecutors say he and his brother, Tamerlan - ethnic Chechens who had lived in the United States for about a decade - carried out the attack in retaliation for U.S. wars in Muslim countries. Tamerlan died in a gunbattle with police.

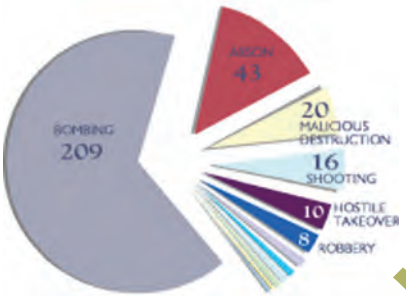
Many Americans view terrorism as an unfortunate by-product of contemporary life. No one knows if the current campaign will be more successful than its predecessors, but we can more fully appreciate the difficulties ahead by examining features of the history of terror. That history shows how deeply implanted terrorism is in our culture, provides parallels worth pondering, and offers a perspective for understanding the uniqueness of September 11 and its aftermath.

I. Terrorism in the United States (An FBI Retrospective: 1980-2005)

Ref: TERRORISM 2002-2005, Federal Bureau of Investigation and Terrorism in the United States 1999, Federal Bureau of Investigation.

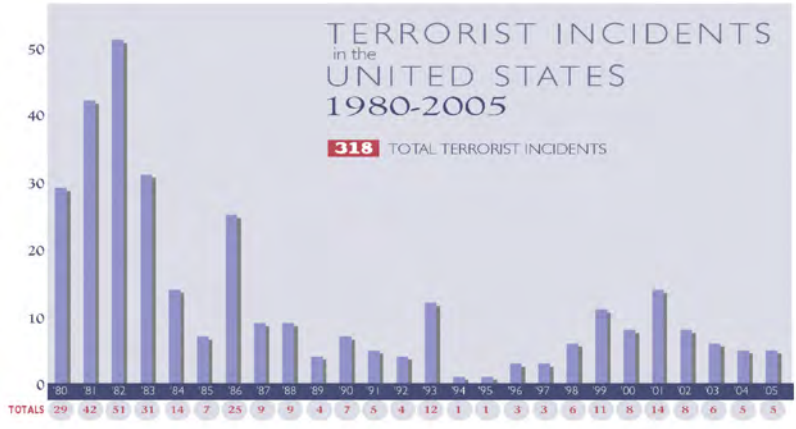
Many Americans view terrorism as an unfortunate by-product of contemporary life. Like oil spills and aircraft disasters, acts of terrorism are considered one of the regrettable–and often inexplicable–perils of modern society. However, terrorism is actually one of the oldest forms of human conflict.

Terrorism in the U.S. Significant Events (1980-2005)



Bombing	209
Arson	43
Malicious Destruction	20
Shooting	16
Hostile Takeover	10
Robbery	8
Assault	4
Hijacking	2
Kidnapping	2
Rocket	2
Assasination	1
WMD	1
TOTAL EVENTS	318

Terrorism is nothing new in the United States; the FBI has been investigating and helping to prevent terrorist attacks since the 1920s. Since the mid-1980s, the FBI has published Terrorism in the United States, an unclassified annual report summarizing terrorist activities in this country. While this publication provided an overview of the terrorist threat in the United States and its territories, its limited scope proved inadequate for conveying either the breadth or width of the terrorist threat facing U.S. interests or the scale of the FBI's response to terrorism worldwide. To better reflect the nature of the threat and the international scope of our response, the FBI expanded the focus of its annual terrorism report in the 2000/2001 edition to include discussion of FBI investigations overseas.



I. Hybrid & Future Threats

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 1 and TRADOC Pamphlet 525-3-1, The U.S. Army Operating Concept: Win in a Complex World 2020-2040 (Oct '14), chap. 2.

I. Hybrid Threats

Hybrid threats are innovative, adaptive, globally connected, networked, and embedded in the clutter of local populations. They can possess a wide range of old, adapted and advanced technologies—including the possibility of weapons of mass destruction (WMD). They can operate conventionally and unconventionally, employing adaptive and asymmetric combinations of traditional, irregular, and criminal tactics and using traditional military capabilities in old and new ways. Understanding hybrid threats involves several key concepts, most of which are not actually new.

Hybrid Threat

A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects.

The term "hybrid" has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. While the existence of innovative adversaries is not new, today's hybrid approaches demand that U.S. forces prepare for a range of conflicts. These may involve nation-state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states.

The emergence of hybrid threats heralds a dangerous development in the capabilities of what was labeled a "guerrilla" or "irregular" force in past conflicts. Hybrid threats can combine state-based, conventional military forces—sophisticated weapons, command and control, and combined arms tactics—with attributes usually associated with insurgent and criminal organizations.

Hybrid threats are characterized by the combination of regular and irregular forces. Regular forces are governed by international law, military tradition, and custom. Irregular forces are unregulated and as a result act with no restrictions on violence or targets for violence. The ability to combine and transition between regular and irregular forces and operations to capitalize on perceived vulnerabilities makes hybrid threats particularly effective. To be a hybrid, these forces cooperate in the context of pursuing their own internal objectives.

Threats can challenge U.S. access—directly and indirectly. They can attack U.S. national and political will with very sophisticated information campaigns as well as seek to conduct physical attacks on the U.S. homeland.

See related discussion of "irregular warfare and insurgencies" on pp. 1-8 to 1-9.

II. Hybrid Threat Components

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 2.

Through formal structure and informal agreement, military and state paramilitary forces can work in concert to varying degrees with insurgent, guerrilla, and criminal groups towards common ends. Typically, the common goal is the removal of U.S. and coalition forces from their area of operations. The goals of hybrid threat forces may or may not coincide with those of other actors in the same geographic area.

Hybrid Threat Components

Threats and Other Actors

A. Nation-State Actors
B. Non-State Actors
C. Regular Military Forces
D. Irregular Forces

Enemy Combatants

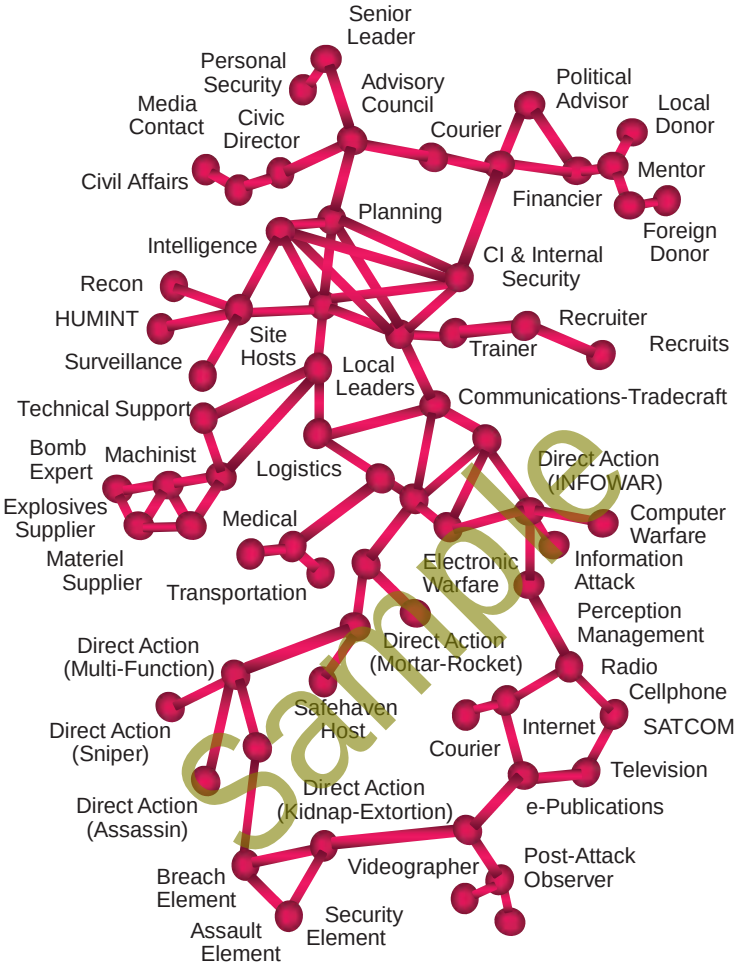
A. Combatants
- Enemy Combatant
- Lawful Enemy Combatant
- Unlawful Enemy Combatant

B. Paramilitary Forces
- Paramilitary
- Insurgent
- Guerrilla
- Terrorist
- Mercenary
- Criminal Organizations

Weapons of Mass Destruction (WMD)

Ref: TC 7-100, Hybrid Threat (Nov '10), chap. 2.

Local Insurgent Organization (Example)



Ref: TC 7-100, Hybrid Threat, fig. 6-1, p. 6-4.

Any relationship of independent local insurgent organizations to regional or national insurgent structures may be one of affiliation or dependent upon a single shared or similar goal. These relationships are generally fluctuating and may be fleeting, mission-dependant, or event- or agenda-oriented. Such relationships can arise and cease due to a variety of reasons or motivations.

When task-organizing insurgent organizations, guerrilla units might be subordinate to a larger insurgent organization. However, they might be only loosely affiliated with an insurgent organization of which they are not a part. A guerrilla unit or other insurgent organization might be affiliated with a regular military organization. A guerrilla unit might also become a subordinate part of an OPFOR task organization based on a regular military unit.

C. Reserves and Militia

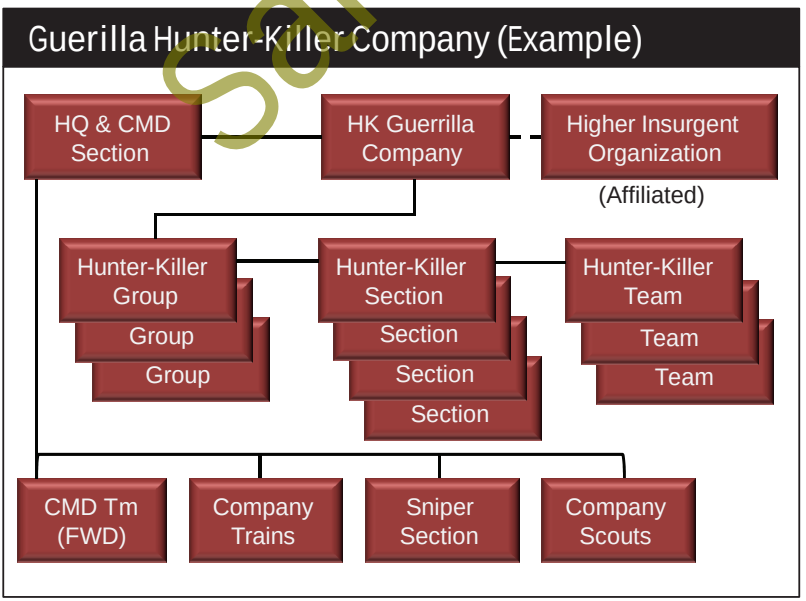
Although all six services can field some reserve forces, most of the reserve forces are Army forces. All militia forces belong to the Army component. Overall planning for mobilization of reserves and militia is the responsibility of the state and its Organization and Mobilization Directorate of the General Staff. Each service component headquarters would have a similar directorate responsible for mobilization of forces within that service. Major geographical commands (and other administrative commands at the operational level and higher) serve as a framework for mobilization of reserve and militia forces.

During mobilization, some reserve personnel serve as individual replacements for combat losses in active units. Others fill positions, including professional and technical specialists, that were left vacant in peacetime in deference to requirements of the civilian sector. However, reservists also man reserve units that are mobilized as units to replace other units that have become combat-ineffective or to provide additional units necessary for large, sustained operations.

Like active force units, most mobilized reserve and militia units do not necessarily go to war under the same administrative headquarters that controlled them in peacetime. Rather, they typically become part of a task-organized operational- or tactical-level fighting command tailored for a particular mission. In most cases, the mobilized reserve units would be integrated with regular military units in such a fighting command. In rare cases, however, a reserve command at division level or higher might become a fighting command or serve as the basis for forming a fighting command based partially or entirely on reserve forces.

III. Guerrilla Organizations

Guerrilla organizations may be as large as several brigades or as small as a platoon or independent hunter-killer (HK) teams. Even in the AFS organizational directories, some guerrilla units were already re-configured as HK units. In the fighting force structure represented in an OPFOR OB, some additional guerrilla units may become task-organized in that manner.



Ref: TC 7-100, Hybrid Threat, fig. 6-2, p. 6-6.

Tactical Concepts

Ref: TC 7-100, Hybrid Threat (Nov '10), pp. 5-1 to 5-3.

Initiative and mobility characterize tactics the HT would use while establishing and preserving bases in which to train, self-sustain, prepare for future missions, and evolve organizational capability. Concurrently, collective tactical actions can have strategic consequences of denying an enemy a secure area or making it politically untenable to remain. Actions are aimed at keeping an enemy physically and psychologically stressed from constant harassment and disruption when a distinct defeat or destruction of an enemy is not practical.

A. Synergy of Regular and Irregular Forces

The HT understands that the environment that would produce the most challenges to U.S. forces is one in which conventional military operations occur in concert with irregular warfare. The HT's concept is not just one of making do with what is available, but is primarily one of deliberately created complexity.

Each component of the HT brings a capability to bear. The synergy of these capabilities is not to be understated. Operational environments (OEs) by their very nature provide a myriad of complexities across all the operational variables. The HT seeks to introduce additional complexity through the use of an ever-shifting array of forces, technologies, and techniques.

B. Information Warfare as a Key Weapon System

HT tactical actions will be often be designed to achieve information warfare (INFOWAR) objectives rather than purely military ones. Information and its management, dissemination, and control have always been critical to the successful conduct of tactical missions. Given today's tremendous advancements in information and information systems technology, this importance is growing in scope, impact, and sophistication. The HT recognizes the unique opportunities that INFOWAR gives tactical commanders. Therefore, it continuously strives to incorporate INFOWAR activities in all tactical missions and battles.

INFOWAR may help degrade or deny effective enemy communications and blur or manipulate the battlefield picture. In addition, INFOWAR helps the HT achieve the goal of dictating the tempo of combat. Using a combination of perception management activities, deception techniques, and electronic warfare (EW), the HT can effectively slow or control the pace of battle. For example, the HT may selectively destroy lucrative enemy targets. It could also orchestrate and execute a perception management activity that weakens the enemy's international and domestic support, causing hesitation or actual failure of the operation. It executes deception plans to confuse the enemy and conceal intentions.

INFOWAR also supports the critical mission of counterreconnaissance at the tactical level. The HT constantly seeks ways to attack, degrade, or manipulate the enemy's reconnaissance, intelligence, surveillance, and target acquisition (RISTA) capabilities. All enemy target acquisition systems and sensors are potential targets.

C. Complex Battle Positions (CBP)

The HT reduces exposure to enemy standoff fires and RISTA by utilizing complex battle positions (CBPs) and cultural standoff. CBPs are designed to protect the units within them from detection and attack while denying their seizure and occupation by the enemy. Commanders occupying CBPs intend to preserve their combat power until conditions permit offensive action. In the case of an attack, CBP defenders will engage only as long as they perceive an ability to defeat aggressors. Should the defending commander feel that his forces are decisively overmatched, he will attempt a withdrawal in order to preserve combat power.

I. Forms of Terrorism (Tactics & Techniques)

Ref: U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), chap. 4; Terrorism in the United States 1999, Federal Bureau of Investigation; and TERRORISM 2002-2005, Federal Bureau of Investigation.

Terrorism is one of the oldest forms of human conflict. Before societies organized to wage war against each other, individuals and small bands engaged in terror tactics to achieve limited goals–to overthrow existing leaders, toward off potential rivals, or to frighten opposing groups from lands they wished to claim for themselves.

(Combating Terrorism Center)

Although the means and ends have evolved throughout history, the central elements of terrorism–fear, panic, violence, and disruption–have changed little through time. As the world enters the 21st Century, terrorism remains a vexing problem–an anachronistic fixture of human relations as paradoxically human and inhuman in the third Millennium as it was before the dawn of recorded history.

If terrorism was not unique to the 20th Century, the remarkable technological and social advances of the second Millennium's closing century created unprecedented opportunities for terrorists, both in terms of the destruction they could create and the level of public anxiety their acts could generate.

The modern era of terrorism–beginning approximately in the late 1960s and continuing through to today–has been the most destructive in history. Over 14,000 international terrorist attacks have taken place worldwide since 1968. These attacks have resulted in more than 10,000 deaths.

While U.S. interests–primarily commercial and diplomatic facilities, U.S.-flagged aircraft, and U.S. nationals–have been a common target for terrorist attacks overseas, U.S. soil remained largely untouched by serious acts of international terrorism until the 1990s, when the World Trade Center bombing and several thwarted plots to

I. Terrorism Trends (Sept. 11, 2001-Present)

Ref: TERRORISM 2002-2005, Federal Bureau of Investigation, pp. 47 to 48.

Beginning in the late 1950s the most serious terrorist threat to U.S. civil aviation came in the form of hijackings of commercial aircraft. In these incidents, the aircraft provided hijackers both transportation to diverted destinations and a ready supply of hostages for leverage in their negotiations with government authorities. By the late 1980s—as seen in the 1988 bombing of Pan Am flight 103 over Lockerbie, Scotland, and in the prevented "Manila Air" plot of 1994—the threat to civil aviation began to include the targeting of commercial aircraft and their passengers and crews for destruction.

On the morning of September 11, 2001, al-Qa'ida directed its ruthless ingenuity toward the further exploitation of civil aviation when 19 of its operatives hijacked four U.S. commercial airliners for use as suicide weapons against selected political, military, and economic targets on the U.S. East Coast. The hijackers used knives, boxcutters, and possibly pepper spray to commandeer the aircraft. Three of the aircraft struck their targets, destroying the Twin Towers of the World Trade Center in New York City and badly damaging the Pentagon in Arlington, Virginia. The fourth aircraft crashed into a remote field in Stonycreek Township, Pennsylvania, as passengers attempted to regain control of the airplane. All of the passengers on each of the aircraft were killed in the attack, as were more than 2,500 people in the Twin Towers and the Pentagon. In total, 2,972 people died in the September 11 attack, making it the most deadly act of terrorism ever committed. The September 11 attack also marked the first known suicide terrorist attack carried out in the United States since the FBI began keeping terrorist records.

The threat of terrorism is expected to continue from both international and domestic sources. Internationally, at least two operational trends are evident in the militant Islamic jihad movement. First is a preference for high-casualty, high-profile attacks directed against lower-risk, unofficial, so-called "soft" targets, as traditional military and diplomatic targets become increasingly hardened. Second, the dissolution of much of al-Qa'ida's structure by international military and law enforcement efforts has resulted in the dispersal of its multinational trainees to pursue their own regional agendas. The following terrorist incidents from September 11, 2001, through 2005 may involve both trends:

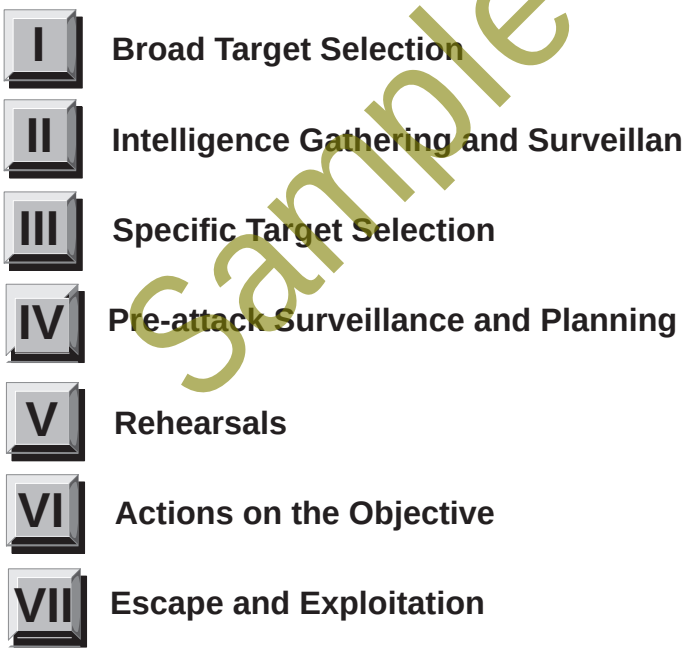
- On October 12, 2002, a nightclub bombing on the Indonesian island of Bali killed approximately 200 people, including seven Americans, and on August 5, 2003, a bombing of the JW Marriott Hotel in Jakarta, Indonesia, resulted in 15 deaths. Both of these bombings have been attributed to members of the Jemaah Islamiyya terrorist organization, a Southeast Asian-based terrorist network with links to al-Qa'ida.
- On May 12 and November 9, 2003, al-Qa'ida operatives conducted bombings of residential compounds that housed Western workers in Riyadh, Saudi Arabia. The first incident claimed dozens of lives and injured nearly 200 others. The second resulted in 18 deaths and over 120 injuries.
- On May 16, 2003, five nearly simultaneous explosions in Casablanca, Morocco, killed 41 people and injured approximately 100 others. Although no definitive evidence links al-Qa'ida to the bombings in Casablanca, the Sunni extremist group responsible for this attack may have al-Qa'ida ties.
- On March 11, 2004, a series of 10 bombs detonated on four commuter trains in Madrid, Spain. The near simultaneous explosions killed 191 people and injured more than 1,400 others. Spanish police have traced responsibility for the attack to Moroccan Islamic militants with ties to al-Qa'ida.

II. Terrorist Planning & Execution

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-17 to II-21, and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), app. A.

Terrorist operations typically are planned in great detail with the objectives of minimizing risk, achieving the highest probability of success, and attaining the widest publicity of their actions. Terrorists seek to avoid adversary strengths and concentrate on their weaknesses. Terrorist tactics are aligned with their overall plans which attempt to use the successful achievement of their operational objectives to realize the accomplishment of their strategic goals. Their approaches to planning and execution follow.

Terrorist Planning Cycle



Ref: JP 3-26, Counterterrorism (Nov '09), fig. II-3, p. II-18.

Terrorist operational planning can be analyzed according to requirements common to all operations. The planning and operation cycle is valid for traditional hierarchically organized groups, as well as decentralized "network" type organizations. The differences between the two organizations are the location of the decision maker at the various steps of the cycle, and the method of task organizing and providing support for the operations.

III. Terrorist Operations & Tactics

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-22 to II-25, and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), chap. 4.

The ensuing discussion presents the most common types of terrorist operations and tactics. It is not intended to be an exhaustive discussion of the subject since the combination of methods and approaches is virtually unlimited. However, common themes in terrorist operations are surprise, secrecy, innovation, and indirect methods of attack. Terrorist tactics are broad and diverse. Additionally, with the use of the Internet and common training bases, terrorist groups exchange information on tactics that can yield success.

Forms of Terrorist Tactics

- **Threat or Hoax**
- **Arson**
- **Sabotage**
- **Bombing**
- **Kidnapping**
- **Hostage Taking**
- **Hijacking**
- **Raid or Ambush**
- **Seizure**
- **Assassination**
- **WMD**
- **Aircraft Threats**
- **Maritime Threats**
- **Suicide Tactics**

Ref: Adapted from JP 3-26, Counterterrorism (Nov '09), fig. II-4, p. II-23.

I. Terrorist Operational Considerations

The terrorist utilizes tactics, forces, and weapons specifically tailored to the particular mission. Terrorist operations are unique, in that each is planned for a specific target and effect. Terrorists normally expose only as much of their resources and personnel as are absolutely necessary to accomplish a mission in order to avoid capture or destruction. A conventional military force would approach an operation with plans to concentrate forces and keep excess combat power on hand to meet contingencies, ensure mission success, and prepare for follow-on missions. A terrorist takes a minimal force and relies upon prior planning and reconnaissance to match the force, weapons, and methods to the target. If changes to the target, or unexpected conditions render success unlikely, the terrorist group will most often cancel or postpone the operation, regroup, update its plan, and adapt to whatever conditions are required to ensure a successful operation. For major terrorist operations, mission accomplishment is often followed by a disbanding of the force, a return of terrorists to their cells and covers, and formation of new task groups for future operations.

In addition to adaptive and flexible organizations, terrorists also employ specific equipment built or procured for a particular operation. Because of the lag time between development of a new technology and military acquisition and fielding, terrorists can sometimes procure equipment superior to standardized military models. As an example, instead of purchasing hundreds of identical radios constructed to meet all likely uses, a terrorist group may only procure the quantity it needs of the

III. Terrorist Methods, Target Types, and Their Psychological Impact

Ref: Dr. Michael A. Bozarth, http://psychologyofterrorism.com (accessed Mar '16).

Difference Between Terror & Terrorism

Terror involves inflicting fear and anxiety on the victim(s) Terror can be goal oriented or gratuitous:

- produce "positive" political, social, economic, or religious change
- extortion for financial gain
- pathological desire to inflict suffering

Terrorism is directed towards "positive" change for a larger group, is seldom 'self-serving' and often 'sacrificing'. Criminal terror benefits the individual, extortion for financial or social gain, and often involves frank or borderline psychopathology.

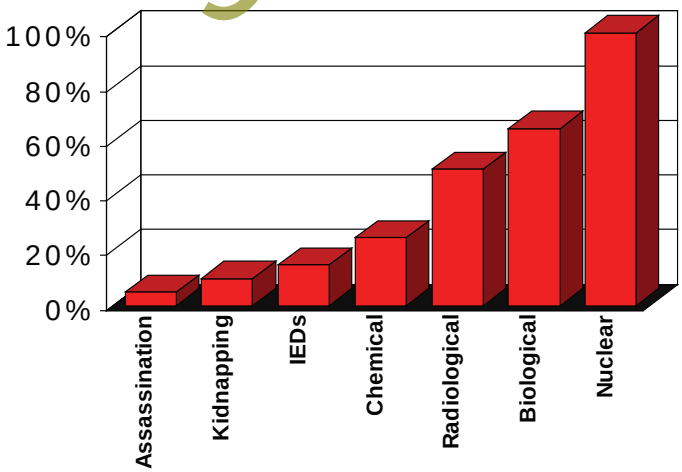
Terrorists seek change through the use of fear and intimidation, but this seldom involves mentally disturbed individuals. Some people use terror gratuitously, and this usually involves mentally disturbed individuals.

Terrorist's Method to Accomplish Goals

A terrorist's method is to instill "terror" in target audience to force capitulation by using the most terrifying means available, including kidnapping, assassination, IEDs, CBRNs by affecting many more people than directly affected by physical actions. Additionally, media and government-response play a critical role in the impact of terrorism.

Terrorist tactics probably work best against democracies, where targeting civilian populations has the greatest effect (i.e., civilians elect the government which sets the policy the terrorists wish to change). In contrast, "soft targets" have little influence on totalitarian government leadership, whereas "hard targets" can erode totalitarian control (through attrition) or even instigate a coup de tat.

Relative Terror Value for Audience Population

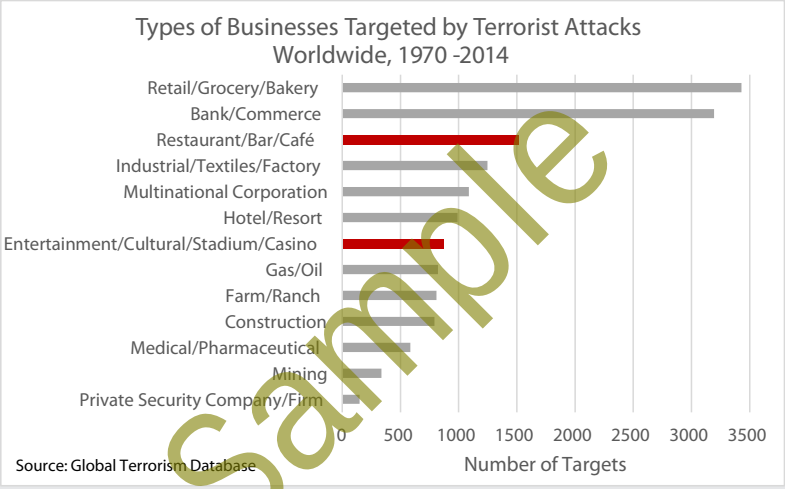


IV. Terrorist Target Venues: Public Places, Businesses, Workplaces

Ref: Miller, Erin. "Mass-Fatality, Coordinated Attacks Worldwide, and Terrorism in France." Background Report, START (2015).

Workplace violence is recognized as a specific category of violent crime that calls for distinct responses from employers, law enforcement, and the community. Contrary to popular opinion, sensational multiple homicides represent a very small number of workplace violence incidents.

The reality -- as evidenced by the tragic events of 9/11, Charlie Hedbo, San Bernandino, and the Paris attacks, just to name a few -- is that a large number of terrorist attacks occur in public venues that are actually workplaces. This brings to light a different perspective of workplace violence than just the traditional law enforcement definition.



The terrorist attacks that occurred in New York, Washington, D.C., and Pennsylvania on September 11, 2001, were a tragic reminder to the Nation of the threat posed by international terrorism. With the exception of the attack on the Pentagon, the targets chosen by the terrorists were not military in nature, but were workplaces where thousands of people work every day to support their families and their country.

Workplace violence was put in a new context that day. Prior to 9/11, this type of violence was viewed as perpetrated by disgruntled employees, customers, or a domestic violence/stalking relationship that surfaces at a workplace.
Since that time, America's workplaces have to be prepared not only to face the more traditional internal workplace threats, but now have to consider the external threat of terrorism.

Robert S. Mueller, III from "Workplace Violence: Issues in Response", 2003
Director of the FBI (2001-2013)

The attacks in Paris reportedly targeted several "soft" targets where large numbers of civilians gather without extraordinary security measures in place. The targets included several restaurants, a theater where a concert was being held, and a sports arena where a soccer match was being held.

IV. Active Shooters & Ideological Homicides

Editor's Note: Although not always classified or perceived as terrorist incidents, the following related topics and special report by the FBI's Critical Incident Response Group (CIRG) and START are presented as related to discussion/examination of terrorism.

I. Active Shooters

Ref: Blair, J. Pete, and Schweit, Katherine W. (2014). A Study of Active Shooter Incidents, 2000 - 2013. Texas State University and Federal Bureau of Investigation, U.S. Department of Justice, Washington D.C. 2014.

Active shooter is a term used by law enforcement to describe a situation in which a shooting is in progress and an aspect of the crime may affect the protocols used in responding to and reacting at the scene of the incident. Unlike a defined crime, such as a murder or mass killing, the active aspect inherently implies that both law enforcement personnel and citizens have the potential to affect the outcome of the event based upon their responses.

(Sept 2013 Washington Navy Yard Shooting/Shane T. McCoy/U.S. Marshals)

The agreed-upon definition of an active shooter by U.S. government agencies—including the White House, U.S. Department of Justice/FBI, U.S. Department of Education, and U.S. Department of Homeland Security/Federal Emergency Management Agency—is "an individual actively engaged in killing or attempting to kill people in a confined and populated area."

(FBI.GOV)

Resolutions

The majority of the 160 incidents (90 [56.3%]) ended on the shooter's initiative—sometimes when the shooter committed suicide or stopped shooting, and other times when the shooter fled the scene.

There were at least 25 incidents where the shooter fled the scene before police arrived. In 4 additional incidents, at least 5 shooters fled the scene and were still at large at the time the study results were released.

In other incidents, it was a combination of actions by citizens and/or law enforcement that ended the shootings. In at least 65 (40.6%) of the 160 incidents, citizen engagement or the shooter committing suicide ended the shooting at the scene before law enforcement arrived.

Of those:

- In 37 incidents (23.1%), the shooter committed suicide at the scene before police arrived.
- In 21 incidents (13.1%), the situation ended after unarmed citizens safely and successfully restrained the shooter. In 2 of those incidents, 3 off-duty law enforcement officers were present and assisted.
- Of note, 11 of the incidents involved unarmed principals, teachers, other school staff and students who confronted shooters to end the threat (9 of those shooters were students).
- In 5 incidents (3.1%), the shooting ended after armed individuals who were not law enforcement personnel exchanged gunfire with the shooters. In these incidents, 3 shooters were killed, 1 was wounded, and 1 committed suicide.
- The individuals involved in these shootings included a citizen with a valid firearms permit and armed security guards at a church, an airline counter, a federally managed museum, and a school board meeting.
- In 2 incidents (1.3%), 2 armed, off-duty police officers engaged the shooters, resulting in the death of the shooters. In 1 of those incidents, the off-duty officer assisted a responding officer to end the threat.

Even when law enforcement arrived quickly, many times the shooter still chose to end his life. In 17 (10.6%) of the 160 incidents, the shooter committed suicide at the scene after law enforcement arrived but before officers could act.

In 45 (28.1%) of the 160 incidents, law enforcement and the shooter exchanged gunfire. Of those 45 incidents, the shooter was killed at the scene in 21, killed at another location in 4, wounded in 9, committed suicide in 9, and surrendered in 2.

V. Media, Disinformation & Radical Propaganda

Ref: JP 3-26, Counterterrorism (Nov '09), pp. II-6, II-25, and V-15 to V-16; and U.S. Army TRADOC G2 Handbook No. 1 (Version 5.0), A Military Guide to Terrorism in the Twenty-First Century (Aug '07), pp. I-2, 5-16 and 5-17.

I. Terrorist IO and Public Relations Activities

Terrorism, like a theatrical play, can be viewed as a deliberate presentation to a large audience in order to gain attention, spotlight a particular message, and seek a response favorable to the actor. The purpose of such actions can have sinister impact on national, regional, and global populations. Global communications provide a stage for near instantaneous media exploitation. Anxiety can increase as random or deliberate acts of terror often target civilians as victims. Similar to a play, the objective of the experience is to affect the feelings and attitudes of the audience.

(Shutterstock.com)

At the fundamental level, terrorism is a psychological act that communicates through the medium of violence or the threat of violence. Terrorist strategies are aimed at publicly causing damage to symbols or inspiring fear. Timing, location, and method of attacks accommodate media dissemination and ensure wide-spread reporting to maximize impact. In its purest form, a terrorist operation often will have the goal of manipulating popular perceptions, and strives to achieve this by controlling or dictating media coverage. This control need not be overt, as terrorists analyze and exploit the dynamics of major media outlets and the pressure of the "news cycle." In considering possible terrorist targets, a massive destructive attack launched against a target that does not attract media coverage may not be a suitable target for the intended effect and targeted population. When the attack is meant to influence a population outside of the area of interest to the terrorists (i.e., the US) in order to influence decision making, a small attack against a "media accessible" target may be a more lucrative target than a larger one of less publicity.

I. National Approach for Counterterrorism

Ref: JP 3-26, Counterterrorism (Oct '14), chap. 3.

The Secretary of Homeland Security is the principal federal official for domestic incident management. The Secretary of Homeland Security coordinates federal operations within the United States to anticipate, prepare for, respond to, and recover from terrorist attacks. The Attorney General of the United States, generally acting through the Director of the Federal Bureau of Investigation (FBI), leads law enforcement response to, and criminal investigations of, terrorist acts or threats within the United States and its territories. The Secretary of Defense (SecDef) may, at the request of the Attorney General, support domestic CT activities and operations. If a terrorist incident exceeds the FBI's capacity, the President may direct DOD to provide domestic CT assistance within Constitutional and statutory limits.

> *"US CT [counterterrorism] efforts require a multidepartmental and multinational effort that goes beyond traditional intelligence, military, and law enforcement functions. We are engaged in a broad, sustained, and integrated campaign that harnesses every tool of American power—military, civilian, and the power of our values—together with the concerted efforts of allies, partners, and multilateral institutions."*
>
> *President Barack Obama, National Strategy for Counterterrorism, June 28, 2011*

I. National Strategy for Counterterrorism

The National Strategy for Counterterrorism formalizes the approach that President Obama and his Administration have been pursuing and adapting to prevent terrorist attacks and to deliver devastating blows against al-Qa'ida, including the successful mission to kill Usama bin Laden.

The latest National Strategy for Counterterrorism was published in June 2011.

For the past decade, the preponderance of the United States' CT effort has been aimed at preventing the recurrence of an attack on the Homeland directed by al-Qa'ida. That includes disrupting plots as well as working to constrain al-Qa'ida's ability to plan and train for attacks by shrinking the size and security of its safehavens.

See the following pages for an overview and fact sheet.

II. National Security Council (NSC)

The National Security Council manages the interagency process with respect to CT and all national security-related issues and certain selected actions. The interagency process is designed to advance the President's policy priorities and to serve the national interest by ensuring that all agencies and perspectives that can contribute to achieving these priorities participate in making and implementing policy. Thus, the National Security Council is the key integrator of the President's whole-of-government CT policy and strategies, which requires interagency coordination at the Principals Committee, Deputies Committee, and supporting interagency policy committees, and the efforts of the National Security Council Staff. The key interagency policy committee of CT is the Counterterrorist Security Group, which is led by the Assistant to the President for Homeland Security and Counterterrorism.

National Strategy for Counterterrorism (Published June 2011)

Ref: Fact Sheet: National Strategy for Counterterrorism, https://www.whitehouse.gov/the-press-office/2011/06/29/fact-sheet-national-strategy-counterterrorism (Accessed Mar 2016).

> *"As a country, we will never tolerate our security being threatened, nor stand idly by when our people have been killed. We will be relentless in defense of our citizens and our friends and allies. We will be true to the values that make us who we are. And on nights like this one, we can say to those families who have lost loved ones to al Qaeda's terror: Justice has been done."*
>
> *--President Barack Obama, May 1, 2011*

The National Strategy for Counterterrorism, found at http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf formalizes the approach that President Obama and his Administration have been pursuing and adapting for the past two and half years to prevent terrorist attacks and to deliver devastating blows against al-Qa'ida, including the successful mission to kill Usama bin Laden.

Rather than defining our entire national security policy, this counterterrorism strategy is one part of President Obama's larger National Security Strategy, which seeks to advance our enduring national security interests, including our security, prosperity, respect for universal values and global cooperation to meet global challenges.

This Strategy builds upon the progress we have made in the decade since 9/11, in partnership with Congress, to build our counterterrorism and homeland security capacity as a nation. It neither represents a wholesale overhaul—nor a wholesale retention—of previous policies and strategies.

Threat

This Strategy recognizes there are numerous nations and groups that support terrorism to oppose U.S. interests, including Iran, Syria, Hezbollah and HAMAS, and we will use the full range of our foreign policy tools to protect the United States against these threats.

However, the principal focus of this counterterrorism strategy is the network that poses the most direct and significant threat to the United States—al-Qa'ida, its affiliates and its adherents.

- **Al-Qa'ida** has murdered thousands of our citizens, including on 9/11.
- Al-Qa'ida **affiliates**—groups that have aligned with al-Qa'ida—have attempted to attack us, such as Yemen-based al-Qa'ida in the Arabian Peninsula's (AQAP) failed attempt to bomb a Detroit-bound airliner on December 25, 2009.
- Al-Qa'ida **adherents**—individuals, sometimes American citizens, who cooperate with or are inspired by al-Qa'ida—have engaged in terrorism, including the tragic slaughter of our service members at Fort Hood in 2009.

Our Ultimate Objective

This Strategy is clear and precise in our ultimate objective: we will disrupt, dismantle, and ultimately defeat al-Qa'ida—its leadership core in the Afghanistan-Pakistan region, its affiliates and adherents to ensure the security of our citizens and interests.

The FBI Counterterrorism Fly Team

Ref: https://www.fbi.gov/about-us/investigate/terrorism/counterterrorism-fly-team

The FBI's Counterterrorism Division Fly Team can respond quickly to dangerous threats and major terrorist attacks around the country and across the globe.

Genesis: On June 21, 2002, the FBI Director announced to Congress the establishment of the Fly Team as a significant counterterrorism initiative under the reorganization plan to refocus the Bureau's mission and priorities following the 9/11 terrorism attacks.

What is it exactly? A small, highly trained cadre of counterterrorism investigators—including special agents and intelligence analysts—based at FBI Headquarters who stand ready to deploy anywhere in the world on a moment's notice.

Fly Team mission: To bring the FBI's strategic and tactical counterterrorism capabilities to bear in partnership with other U.S. government agencies and foreign partner-nation entities in critical overseas locations to detect, penetrate, and disrupt terrorist networks. Specific training and skills include:

- Counterterrorism subject matter expertise
- Advanced interview and interrogation
- Human intelligence operations
- Evidence collection and sensitive site exploitation
- Digital media exploitation and forensics
- Explosive post blast investigations
- Biometrics
- Advanced tactical and force protection skills
- Advanced medical training
- Tactical evasive driving
- Hostage survival and resistance training
- Foreign language skills (Arabic, French, Somali, Spanish)
- Foreign weapons knowledge and proficiency
- Advanced surveillance techniques

How often has the Fly Team been called? Since its creation, the Fly Team has conducted hundreds of strategic deployments throughout the Middle East and North Africa, South Asia, the Horn of Africa, and the war zones of Iraq & Afghanistan. The Fly Team has also responded to numerous counterterrorism critical incidents over the years, with recent examples include the Boston Marathon bombing; Benghazi, Libya – U.S. Consulate Attack; Nairobi, Kenya - Westgate Mall attack; Kampala, Uganda – World Cup bombing; **and** Abuja, Nigeria – Boko Haram kidnapping of school girls.

VI. Global Nature of Counterterrorism Operations

Ref: JP 3-26, Counterterrorism (Oct '14), p. III-5 to III-7.

(Searching Documents/ U.S. Army photo by Spc. Philip Diab)

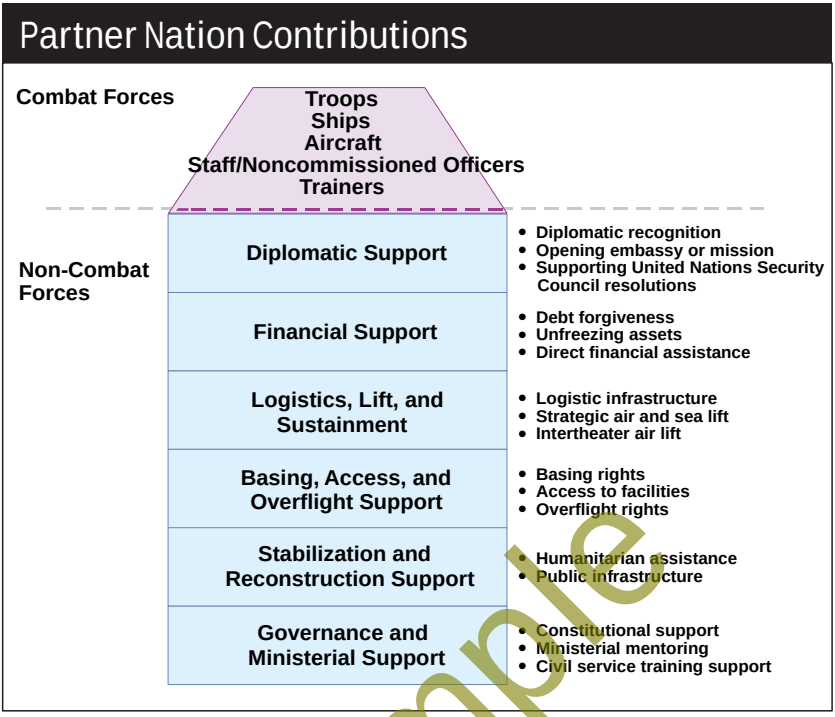
Global SOF Network

All SOF CT forces, whether based in the continental United States (CONUS) or forward-stationed, are part of the global SOF network where all SOF coordinate, exchange information and intelligence, and otherwise synchronize their efforts in support of the GCCs. They are able to connect with cross-functional, multiorganizational entities in CONUS and around the world allowing global collaboration to counter transregional and regional terrorist threats. The key CT organization in each AOR is the TSOC and its subordinate assigned and attached organizations and supporting forces.

Terrorist networks operate in a transnational environment that is not confined by boundaries, borders, or regions. To defeat this type of organization, USSOCOM provides continuous threat monitoring, 24/7 planning and reaction, as directed, and global capabilities that are not confined by department or agency geographic regions.

Partner Nations

DOS engages US partners through the regional levels with regional teams or the subregional level with country teams. DOD works together with DOS and other interagency elements through the GCCs to implement US CT strategy. US strategy against terrorist organizations and individuals associated with terrorist organizations are a mixture of diplomatic, informational, military, and economic options as stated above. The GCC's CT operations are coordinated with allies and integrated into developing foreign partner SOF and conventional forces, and focus on mutual threats to United States and partner sovereignty. PNs' strategies focus on regional threats or adversaries and improving security. Military engagement planning occurs at the country team levels and the CCMD level to support US regional security interests and mitigate PN security concerns.



Ref: JP 3-26 Counterterrorism, fig. III-1, p. III-6.

US CT Strategy with Foreign Partners

US strategy against terrorist organizations and individuals associated with terrorist organizations are a mixture of diplomatic and security options. The US DOD CT enterprise, coordinated with allies and integrated into developing PN SOF, focuses on mutual threats to United States and partner sovereignty.

Military engagement with partners and advising and assisting them to develop CT capabilities are key tools in US CT strategy and leverages SOF regional orientation and expertise that creates an enduring CT partner in the region and often elsewhere.

Indigenous and surrogate forces may be employed to support or conduct CT operations. These indigenous forces may resemble those used during unconventional warfare operations or campaigns. Generally, SOF work with and through irregular forces in unconventional warfare, which are armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces.

Generally, when SOF conduct CT with or through indigenous or surrogate elements, they team with members of the regular armed forces, police forces, or other internal security forces of a PN. A PN may have the national will to apprehend or expel terrorists from inside their borders, but lack the CT resources and expertise to act. Using USG assets to remove terrorists unilaterally from the civilian populace on behalf of a foreign government may present collateral diplomatic, political, and legal risks. In these circumstances, pursuing terrorists with or through regular indigenous forces or surrogates offers several advantages. They generally speak the local language, are sensitive to local culture, and have personal knowledge of the civilian populace. More importantly, they may be legally empowered by their national or local governments to conduct military or law enforcement operations within national borders to impose national will.

maintaining and improving US ability to operate with multinational partners to deter the hostile ambitions of potential aggressors. CT activities during limited contingencies may include intelligence operations to identify terrorists and gain insights into terrorist organizations identified as an imminent threat to a US mission abroad. After terrorists and their organizations are located, CT forces may conduct strikes or raids to neutralize or reduce the threats, and other operations as directed by SecDef or GCC to protect US interests.

C. Major Operations and Campaigns

When required to achieve national strategic objectives or protect national interests, the US national leadership may decide to conduct a major operation or campaign involving large-scale combat. The JFC may employ CT forces in support of all phases of operations to attack adversary state and non-state actors' use of unlawful violence. CT operations in support of major operations and campaigns are sustained and may occur simultaneously in multiple operational areas.

III. Counterterrorism and Types of Activities and Operations

Joint doctrine characterizes the employment of US military by types of activities and operations in order to describe the nature of the effort, tasks, tactics, and other aspects to inform future operations, training, and professional education—CT is a type of operation. There are three broad types of CT activities: advise and assist activities; overseas CT activities; and support to civil authorities activities.

A. Advise and Assist Activities

Advise and assist activities are all US military efforts to improve other nations' ability to provide security for its citizens, govern, provide services, prevent terrorists from using the nation's territory as a safe haven, and promote long-term regional stability.

See facing page for further discussion.

B. Overseas CT Activities

1. Offense, Defense, and Stability Operations

Combat operations vary widely depending on the context of the operation and the objective. Major operations and campaigns, whether or not they involve large-scale combat, will normally include some level of offense, defense, and stability operations. Although defense may be the stronger force posture, it is the offense that is normally decisive in combat. In striving to achieve military strategic objectives quickly and at the least cost, JFCs will normally seek the earliest opportunity to conduct decisive offensive operations. Nevertheless, during sustained offensive operations, selected elements of the joint force may need to pause, defend, resupply, or reconstitute, while other forces continue the attack. Transitioning between offense and defense requires agility. Simultaneously, in many combat operations, the JFC will conduct stability operations to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, or humanitarian relief. The JFC may need to conduct a broad spectrum of CT operations to help secure the population during offensive, defensive, and stability operations.

Stability operations are military missions, tasks, and activities conducted outside the United States, in coordination with other government agencies to maintain or reestablish a safe and secure environment and to provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. The JFC integrates and synchronizes stability operations with other operations within each major operation or campaign phase. Stability operations support USG stabilization

Chap 4

III. Command, Planning & Assessment

Ref: JP 3-26, Counterterrorism (Oct '14), chap. 4.

> *"Now, make no mistake, our nation is still threatened by terrorists… But we have to recognize that the threat has shifted and evolved from the one that came to our shores on 9/11. With a decade of experience now to draw from, this is the moment to ask ourselves hard questions—about the nature of today's threats and how we should confront them."*
>
> *President Barack Obama, National Defense University, May 23, 2013*

I. Command of Counterterrorist Operations

A. General Tenets

1. Command

Command is the exercise of authorities, as specified by SecDef or delegated by a superior JFC, by a properly designated commander over forces assigned or attached to the command. The JP-1, Doctrine for the Armed Forces of the United States, command framework applies to command of CT forces, but because of the unbounded nature of terrorist organizations that operate within and astride GCCs' boundaries, creating a CT command structure that maintains unity of command and achieves unity of action and effort is challenging.

2. Unity of Command

Unity of command means all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose, and no two commanders may exercise the same command relationship over the same force at any one time. The diverse nature of SOF component capabilities and missions, the small size of numerous operational elements that often cross geographically large operations areas, and working with HN forces and/or among indigenous populations make SOF unity of command difficult. The guiding principle is to place all SOF forces under a single JFC with the requisite command authorities and relationships to coordinate special operations among all supporting and supported units. Unless otherwise directed by the President or SecDef, a special operations activity or mission is conducted under the command of the GCC in whose AOR the activity or mission is to be conducted. A GCC normally achieves unity of command of SOF through the CDRTSOC. A commander, joint special operations task force normally provides SOF unity of command for a JFC subordinate to a GCC. CDRTSOC or commander, joint special operations task force, may also be designated the joint force special operations component commander under a JFC.

Also, CDRUSSOCOM must maintain the capability to exercise command of a selected special operations mission if directed by the President or SecDef with the approval of the President.

SecDef may create unity of command across multiple GCC AORs by establishing simultaneous command relationships, such as OPCON, between a CT JFC and multiple GCCs. Each GCC exercises OPCON of the JFC and those CT forces operating in the GCC's AOR; the OPCON does not apply to the JFC's CT forces operating in

other GCCs' AORs. This maintains unity of command because no GCC exercises OPCON of the same forces, only those forces within the GCC's AOR. Furthermore, SecDef, CDRUSSOCOM, or the GCC may enhance unity of command by creating a support command relationship between a supporting CT JFC, not assigned or apportioned to the GCC, and the supported TSOC commander.

3. Unity of Effort and Unified Action

Unity of effort is the coordination and cooperation toward common objectives, as a result of unified action even if the participants are not necessarily part of the same command or organization. Unified action is the synchronized, coordinated, and integrated activities of government and nongovernment entities with those of the military to achieve common objectives. Through unified action CT forces are often employed as part of a whole-of-government effort, operating with other joint forces, various interagency partners, and multinational partners, intergovernmental organizations, NGOs, and HN forces and organizations. This requires the SOF commanders to coordinate and synchronize special operations with other efforts. Unity of effort is an essential complement to unity of command.

B. Command Relationships and Authorities for Counterterrorist Activities and Operations

Title 10, USC, Section 164, is the statutory authority for combatant command (command authority). SecDef, FCCs, GCCs, JFCs, and tactical commanders delegate requisite authorities to subordinate commanders at all levels by establishing command relationships. JP 1, Doctrine for the Armed Forces of the United States, delineates and describes the types of command authority.

Refer to JP 1, Doctrine for the Armed Forces of the United States, for a complete discussion of command authorities, relationships, transfer of forces, and C2.

Counterterrorist Support Command Relationships Establishing Directives

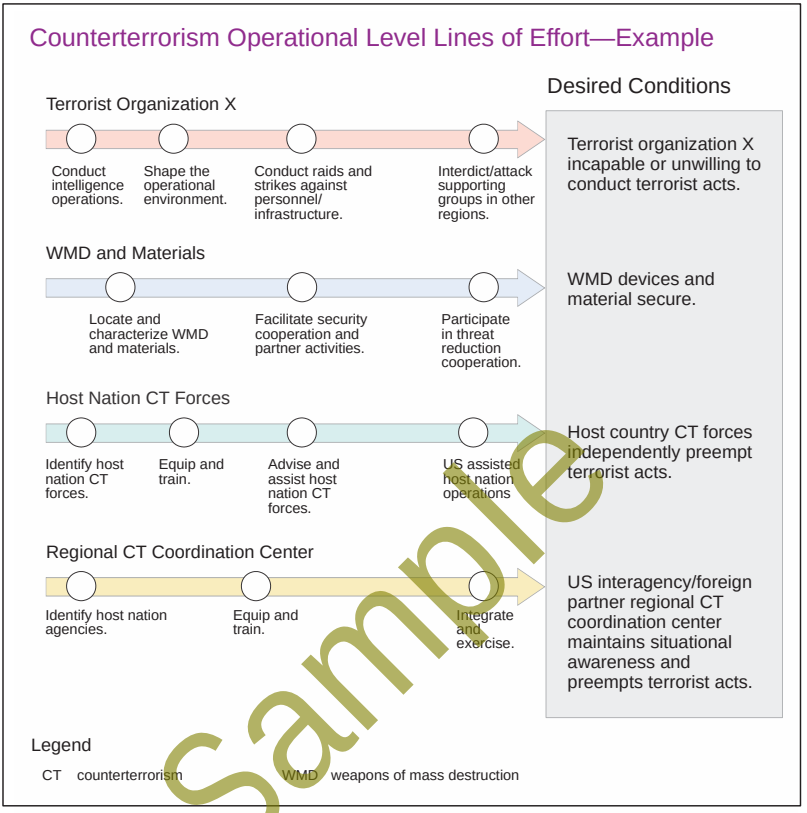
Unless limited by the establishing directive, the supported commander will have the authority to exercise general direction of the supporting effort, including designation and prioritization of targets or objectives, timing and duration of the supporting action, and other instructions necessary for coordination and efficiency.

Unless limited by the establishing directive, the supporting commander has the responsibility to ascertain the needs of the supported commander and take action to fulfill them within existing capabilities, consistent with priorities and requirements of other assigned tasks. The supporting commander determines the forces, tactics, methods, procedures, and communications to be employed in providing this support. The supporting commander will advise and coordinate with the supported commander on matters concerning the employment and limitations (e.g., logistics) of such support, assist in planning for the integration of such support into the supported commander's effort as a whole, and ensure that support requirements are appropriately communicated within the supporting commander's organization.

C. Command Relationships and Assignment and Transfer of Counterterrorist Forces

When a force is assigned, reassigned, or attached, SecDef will specify the command relationship the gaining CCDR will exercise and the losing commander will relinquish. Forces, not command relationships, are transferred between commands. Forces assigned or attached to a CCMD may be further assigned or attached within the CCMD by the CCDR, who will also delegate the appropriate command relationship.

CT operations may combine CT LOEs with those of corresponding DOS, FBI, and other interagency CT partners, which brings to bear capabilities, expertise, and authorities of multiple elements of the USG and facilitates unity of effort when addressing complex CT problems.



Ref: JP 3-26 Counterterrorism, fig. IV-3, p. IV-12.

Commanders synchronize activities along complementary LOOs to achieve the end state.

- **Interior Lines.** A force operates on interior lines when its operations diverge from a central point. Interior lines usually represent central position, where a friendly force can reinforce or concentrate its elements faster than the enemy force can reposition.
- **Exterior Lines.** A force operates on exterior lines when its operations converge on the enemy. Operations on exterior lines offer opportunities to encircle and annihilate an enemy force.

Refer to JFODS4: The Joint Forces Operations & Doctrine SMARTbook (Guide to Joint, Multinational & Interorganizational Operations) for further discussion of the remaining elements of operational design. Topics and chapters include joint doctrine fundamentals, joint operations, joint operation planning, joint logistics, joint task forces, information operations, multinational operations, and interorganizational coordination.

I. Counterterrorist Defeat Mechanism

Ref: JP 3-26, Counterterrorism (Oct '14), p. IV-11 to IV-13.

The defeat mechanism complements the understanding achieved by a COG analysis of a problem by suggesting means to solve it. It is a useful tool to describe the main effects a commander wants to create along a LOO or LOE. The defeat mechanism is to identify, disrupt, isolate, and dismantle terrorist organizations, plus enable HN and PN CT forces that lead to the organization's defeat. Terrorists often reside in remote or inaccessible areas, avoid presenting their organizations to direct attack, blend with populations, and hide their activities until ready to take action. Defeating terrorist organizations requires the application of persistent pressure, eroding their ability to operate, and denying them the ability to instill fear or coerce populations and governments through violence. This requires enduring activities targeting both a terrorist organization's operational capability and its capacity to gain and employ resources. Attacking terrorist organizations requires specifically trained and equipped CT forces, working with interagency partners and independently or with HNs and PNs.

Disrupt

CT disruption is the direct attack of terrorist nodes that are identified during the JIPOE process. All source analysis conducted by specialized intelligence organizations, integrating intelligence provided by USG and PNs, facilitates the identification and targeting of key network nodes. Disruption contributes to degrading terrorist capabilities by eliminating or temporarily neutralizing organizational nodes. Terrorists do not normally mass their forces for engagement, thus CT disruption attacks terrorist nodes to capture or kill terrorists, destroy communications, capture resources, and neutralize materiel required for terrorist acts. The effect of disruption is degradation of the organization's ability to commit acts of terrorism.

Isolate

Isolation limits a terrorist organization's ability to organize, train, plan, or conduct operations effectively by denying communications, resources, recruits, and access to supporting population(s) and/or governments. The effect of isolation is a diminished organization, unable to grow or maintain its size, cutting off logistic support, and eliminating its ability to publicize its cause.

Dismantle

Dismantling exploits the effects of disruption and isolation that further expose the organization to attack. Dismantling may include capturing or killing of remaining key personnel and neutralizing materiel essential to the organization's terrorist capabilities. The effect of dismantling may include dislocation, a shift of terrorist acts to another region or multiple dispersed locations, terrorists unable to acquire recruits or funding to maintain its organization, or members leave the organization for other pursuits.

Enable

Enabling is the advise and assist activities made by US CT forces to ensure HN and PN military and civilian CT forces have sufficient capabilities and capacities to contain or defeat organizations that commit acts of terrorism to further their goals. In addition to providing equipment, training, and operational support, enabling may include sustained military engagement with HN and PN in regional CT coordination centers to maintain situational awareness and to preempt terrorists before they can strike.

IV. Counterterrorism Operations

Ref: JP 3-26, Counterterrorism (Oct '14), chap. 5.

I. Nature of Counterterrorism Operations

Effective CT requires the sustained global CT effort of all relevant USG departments and agencies and PNs, each with unique capabilities, perspectives, and authorities. Over time, by locating and defeating terrorist organizations and networks, they will be rendered incapable or unwilling to use terrorism to achieve their goals. CT activities and operations may support COIN operations, stability operations, or other major operations and campaigns. CT activities and operations are especially useful in irregular warfare to bring military and civilian capabilities to bear in a focused manner against state and non-state actors who use terrorism.

(Dept of Defense Photo)

The DOD core of a global CT enterprise is forces specifically trained and equipped to conduct CT operations against transregional terrorists. An effective CT enterprise is founded upon trust between its members and the ability to work as a team to counter terrorist recruitment, logistics, actions, and planning. The CT enterprise can be decisive when it maintains a sustained look at a terrorist organization globally, uninhibited by USG regional boundaries, rapidly obtains decisions at the national level, and takes action at the tactical level with a speed greater than that of the terrorists. The CT enterprise may take action using a variety of capabilities and authorities, ranging from customs inspection and confiscation, unmanned aerial vehicle strikes, indictment, arrests, and diplomatic consultation to HN action or other USG and foreign efforts.

The ends of CT operations are the elimination of a terrorist's ability or willingness to conduct terrorist acts against the homeland/US facilities and interests abroad or facilitate other terrorist organizations to act against the United States. The ways of CT operations are to capture, kill, or otherwise neutralize terrorist leadership and key subordinates, isolate terrorists from their supporting administrative and logistic infrastructure, and dismantle their capabilities and bases. The means of CT operations are the application of whole-of-government and multinational CT capabilities operating seamlessly through the levels of warfare to disrupt, isolate, and dismantle the nation's most dangerous and difficult terrorist organizations. Additionally, means include influencing relevant populations and impacting the operational environment.

> *"It takes a network to defeat a network...an effective network involves much more than relaying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act."*
>
> *Stanley McChrystal, General, United States Army (Retired), "It Takes a Network," Foreign Policy, February 22, 2011*

Information Operations (IO)

Information operations can create and/or sustain desired and measurable effects on terrorist organizations and networks while protecting and defending the JFC's own forces' actions, information, and information systems. Information-related capabilities such as electronic warfare, cyberspace operations, MISO, and military deception should be applied to CT operations as a means to influence extremists, their supporters, and the mainstream populace. Within an operational area there will be a number of target audiences and there will likely be multiple synchronized themes, messages, and means of delivery required for each. The timing, method, and speed of message delivery will affect which side will gain the upper hand in public opinion. In order to be most effective, narratives and messages should be coordinated among the interagency partners, PNs, and intergovernmental organizations, and should consider NGOs and private sector entities in the operational area.

Counter Threat Finance (CTF) Planning

Counter threat finance (CTF) is an interagency effort to detect, counter, contain, disrupt, deter, or dismantle the transnational financing of state and non-state adversaries threatening US national security. This includes persons and entities that provide financial and material support to terrorists and their networks, including WMD.

In accordance with Title 10, USC, Section 113, Department of Defense Directive 5205.14, DOD Counter Threat Finance (CTF) Policy, establishes DOD policy and assigns DOD responsibilities for the conduct of CTF. CTF is a consideration in all steps of the integrated financial operations process and is a primary concern in evaluation of projects, selection of conduits or implementers, and assessment.

Threat finance intelligence collection, exploitation, analysis, and dissemination of financial information is an essential intelligence support element of CTF activities. Effective CTF requires a global effort. CTF activities include, but are not limited to, countering narcotics trafficking, proliferation activities, WMD networks, trafficking in persons, weapons trafficking, precursor chemical smuggling, terrorist revenue and logistics, anticorruption, and other such activities that generate revenue through illicit networks. It is critical for those conducting CTF to maintain a strong link with financial execution elements. CTF operators must coordinate and share information with those executing integrated financial operations before contracts are approved and funded.

Chap 5

Critical Infrastructure

Ref: NIPP 2013, National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, Dept of Homeland Security (2013) and DCSINT Handbook No. 1.02, Critical Infrastructure (Aug '06).

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy - the infrastructure.

The U.S. has had a wide-reaching Critical Infrastructure Protection Program in place since 1996. The Patriot Act of 2001 defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Since 2009, numerous national policies have continued to shape the way the Nation addresses critical infrastructure security and resilience and national preparedness.

On February 12, 2013, the President issued PPD-21, Critical Infrastructure Security and Resilience, which explicitly calls for the development of an updated national plan. The directive builds on the extensive work done to date to protect critical infrastructure, and describes a national effort to share threat information, reduce vulnerabilities, minimize consequences, and hasten response and recovery efforts related to critical infrastructure. It also identifies 16 critical infrastructure sectors, listed below:

Critical Infrastructure Sectors (16)

- **Chemical**
- **Commercial Facilities**
- **Communications**
- **Critical Manufacturing**
- **Dams**
- **Defense Industrial Base**
- **Emrgency Services**
- **Energy**
- **Financial Services**
- **Government Facilities**
- **Healthcare & Public Health**
- **Information Technology**
- **Nuclear Reactors, Materials, Waste**
- **Transportation Systems**
- **Waste & Wastewater Systems**

Ref: NIPP 2013, National Infrastructure Protection Plan (2013), p. 9.

The President also issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity in February of 2013, which calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing and collaboratively develop and implement risk-based approaches to cybersecurity. The executive order directs the Federal Government to develop a technology-neutral cybersecurity framework to reduce cyber risk to critical infrastructure; promote and incentivize the adoption of strong cybersecurity practices; increase the volume, timeliness, and quality of information sharing related to cyber threats; and incorporate protection for privacy and civil liberties into critical infrastructure security and resilience initiatives.

The National Plan is aligned with the goal of PPD-8, National Preparedness, of "a secure and resilient Nation with the capabilities required across the whole communi-

I. The Protection Challenge

Ref: National Strategy for Physical Protection of Critical Infrastructure and Key Assets (Feb '03), p. viii and p. 9.

The Importance of Critical Infrastructures

America's critical infrastructure sectors provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose. Critical infrastructures frame our daily lives and enable us to enjoy one of the highest overall standards of living in the world.

The facilities, systems, and functions that comprise our critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function.

The Importance of Key Assets

Key assets and high profile events are individual targets whose attack—in the worst-case scenarios—could result in not only large-scale human casualties and property destruction, but also profound damage to our national prestige, morale, and confidence

Individually, key assets like nuclear power plants and dams may not be vital to the continuity of critical services at the national level. However, a successful strike against such targets may result in a significant loss of life and property in addition to long-term, adverse public health and safety consequences. Other key assets are symbolically equated with traditional American values and institutions or U.S. political and economic power. Our national icons, monuments, and historical attractions preserve history, honor achievements, and represent the natural grandeur of our country. They celebrate our American ideals and way of life and present attractive targets for terrorists, particularly when coupled with high profile events and celebratory activities that bring together significant numbers of people.

The Protection Challenge

Agriculture and Food	1,912,000 farms; 87,000 food-processing plants
Water	1,800 federal reservoirs; 1,600 municipal waste water facilities
Public Health	5,800 registered hospitals
Emergency Services	87,000 U.S. localities
Defense Industrial Base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	
Electricity	2,800 power plants
Oil and Natural Gas	300,000 producing sites
Transportation	
Aviation	5,000 public airports
Passenger Rail and Railroads	120,000 miles of major railroads
Highways, Trucking, and Busing	590,000 highway bridges
Pipelines	2 million miles of pipelines
Maritime	300 inland/costal ports
Mass Transit	500 major urban public transit operators
Banking and Finance	26,600 FDIC insured institutions
Chemical Industry and Hazardous Materials	66,000 chemical plants
Postal and Shipping	137 million delivery sites
Key Assets	
National Monuments and Icons	5,800 historic buildings
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Government Facilities	3,000 government owned/operated facilities
Commercial Assets	460 skyscrapers

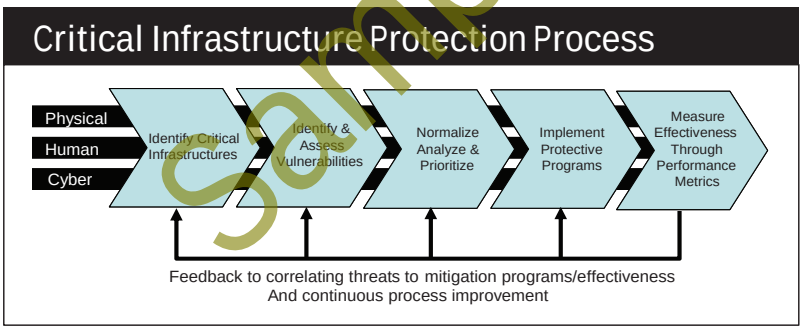
**These are approximate figures.*

I. Identifying Vulnerabilities in Critical Infrastructure

Ref: DCSINT Handbook No. 1.02, Critical Infrastructure (Aug '06), section III.

> *"The War against America and its allies will not be confined to Iraq…As for similar operations taking place in America; it's only a matter of time. They are in the planning stages, and you will see them in the heart of your land as soon as the planning is complete"*
>
> *Osama Bin Laden, al-Jazeera, 19 January 2006*

The definition of critical infrastructure has been given and examples of the critical infrastructures of the United States are provided, but what are our critical infrastructures within our own areas of responsibility, influence and interest? Some of these are provided to us by our higher organizations and their commands. Those higher infrastructures and parts of infrastructures located in our areas of responsibility are listed to us and we ensure their protection. These areas can be labeled Mission Essential Vulnerable Areas (MEVAs). Unfortunately a list of critical infrastructures and sites is not always provided; oftentimes staffs have to decide what are their critical infrastructures and the key assets supporting them. The staff or command will need to understand the infrastructures, how they function and which parts they need to protect.



Ref: DCSINT HNDBK 1.02 Critical Infrastructure, flowchart, p. III-4.

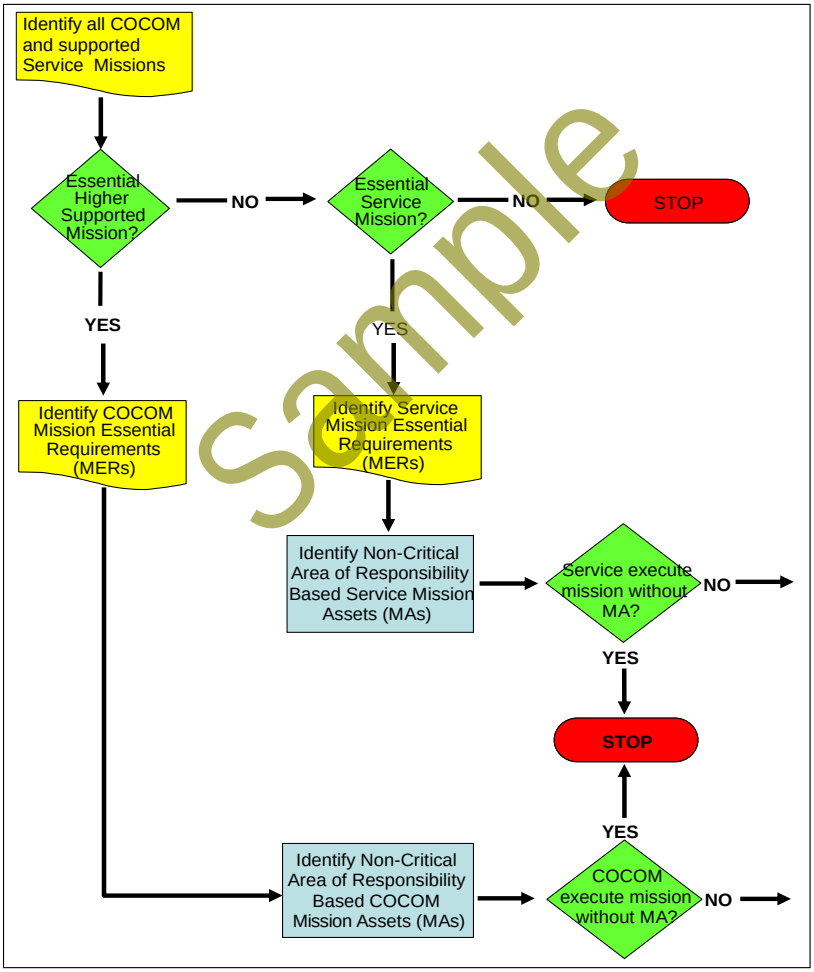
On the following two pages is a flow chart designed to assist in the understanding of what is critical and the weaknesses within those systems. The flow chart was designed by NORTHCOM's J34, Assessments Branch, to assist units and organizations in looking at themselves, their missions and to identify weaknesses and single points of failure within the infrastructures.

The process starts with identifying all of the missions the higher headquarters has directed the unit to perform as well as those functions the higher headquarters perform that are located within the unit's area of responsibility. The staff works their way through the process identifying missions and requirements at their own level, their higher's level as well as those they support, and decide if each are critical. When the staff reaches the end of the process they must conduct a Dependency Analysis in an effort to identify Single Points of Failure (SPOF). These SPOFs are the likely targets of attack as they will result in most damage for the least expenditure.

I. CIP Assessment Flow Chart

Ref: DCSINT Handbook No. 1.02, Critical Infrastructure (Aug '06), pp. III-1 to III-6.

The process is designed to help garrisons and staffs to determine what are their critical infrastructures and where are they vulnerable. These vulnerabilities are above and beyond those single points of failure that a higher office or headquarters may already have identified as critical to their operations but the physical asset is located on the lower headquarters facility or post. The list of critical infrastructures and their vulnerabilities, those of each level of command, must be nested together so that the individuals responsible for the security of the installation know the entire lists of assets that must be secured. Simply put, what is critical to one person or level of command might not be critical to another, but those responsible for the security where the critical asset resides must know it is critical in order to protect and secure it. The nesting of these various layers can only be insured through coordination and synchronization between all levels of command. Once a list of assets and single points of failure exists it must be updated as plans and priorities change.



Ref: DCSINT HDBK 1.02 Critical Infrastructure. flowchart. p. III-2.

II. Critical Infrastructure Risk Management

Ref: NIPP 2013, National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, Dept of Homeland Security (2013), pp. 15-20.

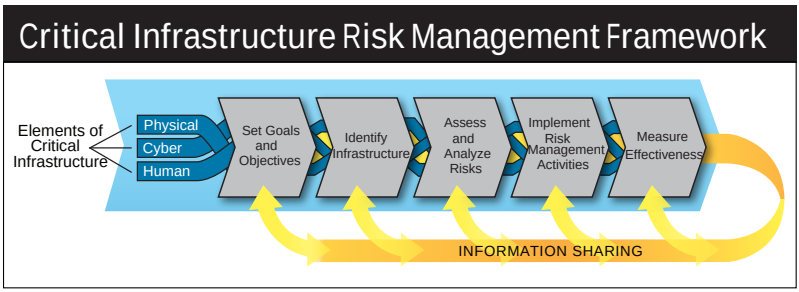
The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private sector critical infrastructure owners and operators to make risk-informed decisions on the most effective solutions available when allocating limited resources in both steady-state and crisis operations.

Risk management enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm, and employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration.

RM, as it is discussed in terms of critical infrastructure, is not to be confused with Operational Risk Management (ORM). ORM methods are applied during the course of military operations and are focused on improving safety for personnel engaged in those operations. RM is focused on reducing risks to the installation and its critical assets.

I. CI Risk Management Framework

Critical infrastructure partners manage risks based on diverse commitments to community, focus on customer welfare, and corporate governance structures. Risk tolerances will vary from organization to organization, as well as sector to sector, depending on business plans, resources, operating structure, and regulatory environments. They also differ between the private sector and the government based on underlying constraints. Different entities are likely to have different priorities with respect to security investment as well as potentially differing judgments as to what the appropriate point of risk tolerance may be. Private sector organizations generally can increase investments to meet their risk tolerances and provide for their community of stakeholders, but investments in security and resilience have legitimate limits. The government must provide for national security and public safety and operates with a different set of limits in doing so.



Ref: NIPP 2013, National Infrastructure Protection Plan (2013), fig. 3, p. 15.

The critical infrastructure risk management framework supports a decision-making process that critical infrastructure partners collaboratively undertake to inform the selection of risk management actions. This framework is not binding and many organizations have risk management models that have proved effective and should be maintained. It does, however, provide an organizing construct for those models.

A. Set Infrastructure Goals and Objectives

This National Plan establishes a set of broad national goals for critical infrastructure security and resilience. These national goals are supported by objectives and priorities developed at the sector level, which may be articulated in Sector-Specific Plans (SSPs) and serve as targets for collaborative planning among SSAs and their sector partners in government and the private sector.

A set of national multi-year priorities, developed with input from all levels of the partnership, will complement these goals. These priorities might focus on particular goals or cross-sector issues where attention and resources could be applied within the critical infrastructure community with the most significant impact. Critical infrastructure owners and operators, as well as SLTT and regional entities, can identify objectives and priorities for critical infrastructure that align to these national priorities, national goals, and sector objectives, but are tailored and scaled to their operational and risk environments and available resources.

B. Identify Infrastructure

To manage critical infrastructure risk effectively, partners must identify the assets, systems, and networks that are essential to their continued operation, considering associated dependencies and interdependencies. This aspect of the risk management process also should identify information and communications technologies that facilitate the provision of essential services.

Critical infrastructure partners view criticality differently, based on their unique situations, operating models, and associated risks. The Federal Government identifies and prioritizes nationally significant critical infrastructure based upon statutory definition and national considerations. SLTT governments identify and prioritize infrastructure according to their business and operating environments and associated risks. Infrastructure owners and operators identify assets, systems, and networks that are essential to their continued operations and delivery of products and services to customers. At the sector level, many SSAs collaborate with owners and operators and SLTT entities to develop lists of infrastructure that are significant at the national, regional, and local levels.

Effective risk management requires an understanding of criticality as well as the associated interdependencies of infrastructure. This National Plan identifies certain lifeline functions that are essential to the operation of most critical infrastructure sectors. These lifeline functions include communications, energy, transportation, and water. Critical infrastructure partners should identify essential functions and resources that impact their businesses and communities. The identification of these lifeline functions can support preparedness planning and capability development.

C. Assess and Analyze Risks

Critical infrastructure risks can be assessed in terms of the following:

- **Threat** – natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability** – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- **Consequence** – effect of an event, incident, or occurrence.

Risk assessments are conducted by many critical infrastructure partners to inform their own decision making, using a broad range of methodologies. These assessments allow critical infrastructure community leaders to understand the most likely and severe incidents that could affect their operations and communities and use this information to support planning and resource allocation in a coordinated manner.

III. Cyber Threats & Cyber-Terrorism

Ref: JP 3-12 (Redacted), Cyberspace Operations (Feb 13); DCSINT Handbook No. 1.02, Critical Infrastructure (Aug '06), section VII; and US Air Force Doctrine, Annex 3-12, Cyberspace Operations, updated 30 Nov 2011. (Compiled by Jay Martin.)

Civilian, commercial and government networks are probed millions of times per day and are routinely the victims of intrusion, exploitation, and low-level computer attack. Often, hackers gain and maintain access to systems, even those thought to be off the network, for periods of more than a year before the victims even realize their systems have been compromised. This access provides the potential for damaging and even catastrophic attacks.

(Shutterstock.com)

I. Cyberspace Attacks

Cyberspace attacks come in many forms and can range from obvious to non-obvious. Cyber attacks that clearly deny (degrade, disrupt, or destroy) a network are obvious. The most troublesome attacks, however are not obvious and may involve the manipulation of data. When these attacks are detected, they can cast doubt on the integrity of the entire network. Still, other attacks involve the exfiltration and exploitation of data, sometimes revealing plans or capabilities and undermining mission success.

A cyber attacker possesses inherent advantages over a defender. In contrast to land warfare, in cyberspace the concept of a culminating point does not apply. The cyber attacker does not tire nor expend resources. His lines of communication do not require sustainment or protection, and he usually has multiple avenues of approach. In fact the cyber attacker may get stronger as he penetrates defenses and finds it

easier to sustain the attack. The more cyber attackers the enemy employs, both human and machine, the greater their chances of success.

Several studies examining the cyber threat have shown that critical infrastructures are potential targets of cyber terrorists. These infrastructures make extensive use of computer hardware, software, and communications systems. However, the same systems that have enhanced their performance potentially make them more vulnerable to disruption by both physical and cyber attacks to these IT systems. These infrastructures include:

- Energy systems
- Emergency services
- Telecommunication
- Banking and finance
- Transportation
- Water system

A quick review of the automation used in the electric power industry demonstrates the potential vulnerabilities to our critical infrastructures. The electrical industry has capitalized on computer technology for improved communication and automation of control centers, substations and remote protection equipment. They use a host of computer-based equipment including SCADA systems; substation controllers consisting of programmable logic controllers, remote terminal units, data processing units and communication processors; and intelligent electronic devices consisting of microprocessor-controlled meters, relays, circuit breakers, and circuit reclosers.

Although there have been no major terrorist attacks to these critical infrastructure systems to date, there is evidence that terrorist groups have been conducting surveillance on them. As stated earlier in this section under “Research,” police have found a pattern of surveillance by unknown browsers located in the Middle East and South Asia against emergency telephone systems, electrical generation and transmission facilities, water storage and distribution systems, nuclear power plants, and gas facilities.

Although these systems fall within the civilian sector, the military is highly dependent on all of these critical functions and would be directly impacted if they were successfully attacked. Consider the impact on unit deployment if a successful cyber attack, or a combination of cyber and physical attack, is conducted against our critical infrastructure during movement—

- Disruption of the rail system could severely impact movement of equipment to a port of embarkation
- A successful attack against a power substation could halt loading operations at the port
- A successful attack against the telecommunications systems would directly impact the command and control of the operations

II. Cyber-Terrorism

Cyber-terrorism is a development of terrorist capabilities provided by new technologies and networked organizations, which allows terrorists to conduct their operations with little or no physical risk to themselves. Cyber-terrorism is a new and somewhat nebulous concept, with debate as to whether it is a separate phenomenon, or just a facet of information warfare practiced by terrorists. Even for those that believe cyber-terrorism is a separate phenomenon; the boundaries often become blurred between information warfare, computer crime, online social activism, and cyber-terrorism.

Cyber-terrorism differs from other improvements in terrorist technology because it involves offensive information technology capabilities, either alone or in combination with other forms of attack. Some examinations of cyber-terrorism focus on the physi-

I. Protection Warfighting Function

Ref: ADP 3-37, Protection (Aug '12) and ADRP 3-0, Unified Land Operations (May '12), pp. 3-5 to 3-6. See also p. 1-41.

Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0).

Commanders and staffs synchronize, integrate, and organize capabilities and resources throughout the operations process to preserve combat power and the freedom of action and to mitigate the effects of threats and hazards. Protection safeguards the force, personnel (combatants and noncombatants), systems, and physical assets of the United States and unified action partners. Survivability refers to the capacity, fitness, or tendency to remain alive or in existence. For the military, survivability is about much more than mere survival—it is also about remaining effective. Military forces are composed of personnel and physical assets, each having their own inherent survivability qualities or capabilities that permit them to avoid or withstand hostile actions or environmental conditions while retaining the ability to fulfill their primary mission.

I. The Protection Warfighting Function

The protection warfighting function is the related tasks and systems that preserve the force so that commanders can apply maximum combat power to accomplish the mission (ADRP 3-0). Preserving the force includes protecting personnel (combatants and noncombatants), systems, and physical assets of the United States and unified action partners. The protection warfighting function enables commanders to preserve force integrity and combat power by integrating protection capabilities to safeguard bases/base camps, secure routes, and protect forces. Commanders incorporate protection when they understand and visualize capabilities available for protection. Some of these actions or effects may be achieved through the combined integration of the eight elements of combat power, resulting in an increasingly effective and efficient scheme of protection.

The supporting tasks of the protection warfighting function are—

- Conduct operational area security
- Employ safety techniques (including fratricide avoidance)
- Implement operations security
- Provide intelligence support to protection
- Implement physical security procedures
- Apply antiterrorism measures
- Conduct law and order
- Conduct survivability operations
- Provide force health protection
- Conduct chemical, biological, radiological, and nuclear operations
- Provide explosive ordnance disposal and protection support
- Coordinate air and missile defense
- Conduct personnel recovery operations
- Conduct internment and resettlement

Refer to JP 3-0 for more information on joint protection tasks.

II. The Role of Protection

Ref: ADP 3-37, Protection (Aug '12), pp. 1 to 2.

Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area (Joint Publication [JP] 3-0). Commanders and staffs synchronize, integrate, and organize capabilities and resources throughout the operations process to preserve combat power and mitigate the effects of threats and hazards. Protection is a continuing activity; it integrates all protection capabilities to safeguard the force, personnel (combatants and noncombatants), systems, and physical assets of the United States and unified action partners.

Operational environments are uncertain, marked by rapid change and a wide range of threats and hazards. These evolving operational environments will provide significant challenges for commanders and staffs who are integrating protection capabilities. Protection preserves the combat power potential of the force by providing capabilities to identify and prevent threats and hazards and to mitigate their effects. Army units may also be required to provide protection for civilians in order to support mission objectives. This may include protecting civilians from widespread violence (such as mass atrocities), mitigating civilian casualties, and ensuring a secure environment for the population and nonmilitary partners.

Protection can be maximized by integrating the elements of combat power to reinforce protection or to achieve complementary protective effects. The goal of protection integration is to balance protection with the freedom of action throughout the duration of military operations. This is accomplished by integrating reinforcing or complementary protection capabilities into operations until all significant vulnerabilities have been mitigated, have been eliminated, or become assumed risks. The employment of synchronized and integrated reinforcing and complementary protection capabilities preserves combat power and provides flexibility across the range of military operations. The collaboration, integration, and synchronization between the warfighting functions assist in identifying and preventing threats and hazards and in mitigating their effects.

Army leaders are responsible for clearly articulating their visualization of operations in time, space, purpose, and resources. The commander's inherent responsibility to protect and preserve the force and secure the area of operations is vital in seizing, retaining, and exploiting the initiative. Protection must be considered throughout the operations process to—

- Identify threats and hazards
- Implement control measures to prevent or mitigate enemy or adversary actions
- Manage capabilities to mitigate the effects and time to react or maneuver on the adversary to gain superiority and retain the initiative

A shared understanding and purpose of the joint protection function (see JP 3-0) allows Army leaders to integrate actions within the unified action and to synchronize operations. The joint protection function focuses on preserving the joint force fighting potential in four primary ways:

- **Active defensive measures** to protect the joint force, its information, its bases/base camps, critical infrastructure, and lines of communications from an enemy or adversary attack
- **Passive defensive measures** to make friendly forces, systems, and facilities difficult to locate, strike, and destroy
- The application of technology and procedures to **reduce the risk of fratricide**
- **Emergency management and response** to reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters

C. Implement Operations Security (OPSEC)

Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities (JP 3-13.3). OPSEC may also be used to—

- Identify actions that can be observed by enemy or adversary intelligence systems
- Determine indicators of hostile intelligence that systems might obtain which could be interpreted or pieced together to derive critical information in time to be useful to adversaries or enemies
- Execute measures that eliminate or reduce (to an acceptable level) the vulnerabilities of friendly actions to enemy or adversary exploitation

OPSEC applies to all operations. All units conduct OPSEC to preserve essential secrecy. Commanders establish routine OPSEC measures in unit standing operating procedures. The unit OPSEC officer coordinates additional OPSEC measures with other staff and command elements and synchronizes with adjacent units. The OPSEC officer develops OPSEC measures during the military decisionmaking process. The assistant chief of staff, intelligence, assists the OPSEC process by comparing friendly OPSEC indicators with enemy or adversary intelligence collection capabilities.

Refer to JP 3-13.3 for additional OPSEC information.

D. Provide Intelligence Support to Protection

This is an intelligence warfighting function task that supports the protection warfighting function. It includes providing intelligence that supports measures which the command takes to remain viable and functional by protecting itself from the effects of threat activities. It also provides intelligence that supports recovery from threat actions. It includes analyzing the threats, hazards, and other aspects of an operational environment and utilizing the intelligence preparation of the battlefield process to describe the operational environment and identify threats and hazards that may impact protection. Intelligence support develops and sustains an understanding of the enemy, terrain and weather, and civil considerations that affect the operational environment. Information collection is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations (FM 3-55). Information collection can complement or supplement protection tasks. Through information collection, commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information to satisfy the commander's critical information requirements and other intelligence requirements. When necessary, information collection assets (ground- and space-based reconnaissance and surveillance activities) focus on special requirements, such as personnel recovery.

Refer to ADRP 2-0 for additional intelligence information.

E. Apply Antiterrorism (AT) Measures

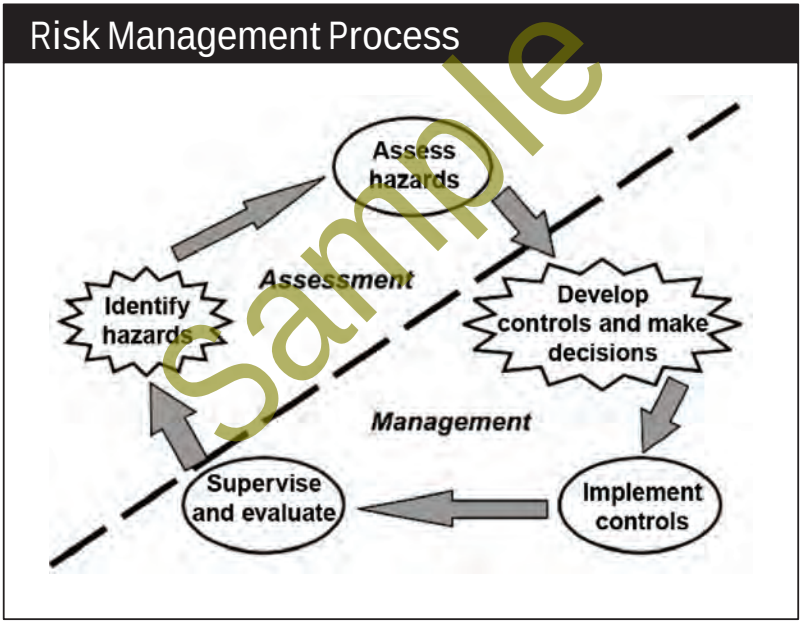
AT consists of defensive measures that are used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. AT is a consideration for all forces during all military operations.

AT is an integral part of Army efforts to defeat terrorism. Terrorists can target Army elements at any time and in any location. By effectively preventing and, if necessary, responding to terrorist attacks, commanders protect all activities and people so that Army missions can proceed unimpeded. AT is neither a discrete task nor the sole responsibility of a single branch; all bear responsibility. AT must be integrated into all Army operations and considered at all times. Awareness must be built into every mission, every Soldier, and every leader. Integrating AT represents the foundation that is crucial for Army success.

III. Protection Planning

Ref: ADRP 3-37 (FM 3-37), Protection (Aug '12), chap. 2. See also p. 7-6.

Planning is the first step toward effective protection. Commanders consider the most likely threats and hazards and then decide which personnel, physical assets, and information to protect. They set protection priorities for each phase or critical event of an operation. The military decisionmaking process or troop leading procedures provide a deliberate process and context to develop and examine information for use in the various continuing activities and integrating processes that comprise the operations process. An effective scheme of protection and risk decisions are developed based on the information that flows from mission analysis, allowing a thorough understanding of the situation, mission, and environment. Mission analysis provides a context to identify and analyze threats and hazards, the situational understanding of the operational environment, and the development of the scheme of protection.



Ref: ADRP 3-37, Protection, fig. 2-1, p. 2-2.

I. Initial Assessments

Initial protection planning requires various assessments to support protection prioritization; namely, threat, hazard, vulnerability, criticality, and capability. These assessments are used to determine which assets can be protected given no constraints (critical assets) and which assets can be protected with available resources (defended assets). Commanders make decisions on acceptable risks and provide guidance to the staff so that they can employ protection capabilities based on the CAL and DAL. All forms of protection are utilized and employed during preparation and continue through execution to reduce friendly vulnerability.

Initial Assessments (Protection)

Threat and Hazard Assessment *(p. 6-26)*

Vulnerability Assessment *(p. 6-28)*

Criticality Assessement *(p. 6-28)*

Capability Assessement *(p. 6-29)*

Ref: ADRP 3-37, Protection, chap. 2.

II. Integrating Processes

The integrating processes of intelligence preparation of the battlefield, targeting, and risk management are essential in providing assessments or key information to assessments. They are a vital part of integrating protection within the other warfighting functions and throughout the operations process.

Intelligence Preparation of the Battlefield (IPB)

The intelligence preparation of the battlefield is a systematic process of analyzing and visualizing the mission variables of threat, terrain, weather, and civil considerations in a specific area of interest and for a specific mission. By applying the intelligence preparation of the battlefield, commanders gain the information necessary to selectively apply and maximize operation effectiveness at critical points in time and space.

Targeting

The targeting process integrates commander guidance and priorities to determine which targets to engage and how, when, and where to engage them in order to assign friendly capabilities to achieve the desired effect. The staff then assigns friendly capabilities that are best suited to produce the desired effect on each target. An important part of targeting is identifying possibilities for fratricide and collateral damage. Commanders establish control measures, including the consideration for restraint, that are necessary to minimize the chance of these events. The protection priorities must be integrated within the targeting process to achieve the desired effects while ensuring the preservation of combat power.

Risk Management

Risk management is the process of identifying, assessing, and controlling risks that arise from operational factors and making decisions that balance risk cost with mission benefits. Threat, hazard, capability, vulnerability, and criticality assessments are utilized to evaluate the risk to the force, determine the critical assets, ascertain available resources, and apply security or defensive measures to achieve protection. Risk management helps commanders preserve lives and resources, avoid or mitigate unnecessary risk, identify and implement feasible and effective control measures where specific standards do not exist, and develop valid courses of action (COAs). Risk management integration during operations process activities is the primary responsibility of the unit protection officer or operations officer.

See fig. 2-1 on previous page for an overview of the risk management process.

Chap 7

I. Countering Weapons of Mass Destruction

Ref: JP 3-40, Countering Weapons of Mass Destruction (Oct '14), chap. 1.

I. General

Weapons of mass destruction (WMD) are chemical, biological, radiological, or nuclear weapons or devices capable of a high order of destruction and/or causing mass casualties. This does not include the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon. WMD does not include high-yield explosives. The existence of chemical, biological, radiological, and nuclear (CBRN) materials and the potential for use by actors of concern precipitates the need to plan, prepare for, and counter their use.

(FBI.GOV)

Countering weapons of mass destruction (CWMD) entails activities across the United States Government (USG) to ensure the US, its Armed Forces, allies, partners, and interests are not attacked or coerced by actors of concern possessing WMD. CWMD is a national security priority.

> *"The gravest danger to the American people and global security continues to come from weapons of mass destruction, particularly nuclear weapons."*
>
> *National Security Strategy, May 2010*

Actors of Concern

Actors of concern are those state or non-state actors that carry out activities that, left unaddressed, pose a clear threat to the strategic objectives of the USG. Actor of concern's possession of WMD, proliferation of WMD, and the pursuit of WMD by extremists present grave threats to the American people. Actors of concern with WMD possess an asymmetric advantage capable of significantly neutralizing the superior technology, military, and economic strength of the US and its allies. CWMD is a continuous campaign that requires a coordinated, whole-of-government effort to curtail the conceptualization, development, possession, proliferation, use, and effects of WMD-related expertise, materials, and technologies.

The Department of Defense (DOD) contributes to this whole-of-government effort by providing joint forces that plan and execute tasks to ensure that the US, its forces, allies, partners, and interests are neither coerced nor attacked with WMD. These joint forces also prepare for the execution of contingency responses to WMD-related crises. The world events that define the WMD problem have evolved over time. With the advent of US conventional military preeminence and continued improvements in US missile defenses and capabilities to counter and mitigate the effects of WMD, the role of US nuclear weapons in deterring nonnuclear attacks—conventional, biological, or chemical—has declined. To that end, US declaratory policy is not to use or threaten to use nuclear weapons against nonnuclear weapons states that are party to the Treaty on the Nonproliferation of Nuclear Weapons (NPT) and in compliance with their nuclear nonproliferation obligations. In making this declaration, the US affirms that any state eligible for the assurance that uses chemical or biological weapons against the US or its allies and partners would face a devastating conventional military response. Given the catastrophic potential of biological weapons and the rapid pace of biotechnology development, the US reserves the right to make any adjustment in the assurance that may be warranted by the evolution and proliferation of the biological weapons threat and US capacities to counter that threat. In the case of states that possess nuclear weapons and states not in compliance with nuclear nonproliferation obligations there remains a narrow range of contingencies in which US nuclear weapons may be employed in deterring a conventional or WMD attack.

II. National Strategy and Guidance

National guidance provides the foundation for the development of DOD CWMD strategy and guidance documents. Top-level strategy and general guidance for CWMD is derived from the National Security Strategy (NSS) and WMD-specific Presidential decision directives (e.g., national security Presidential directives [NSPDs] and Presidential policy directives [PPDs]). b. Unified Command Plan (UCP). The UCP is Presidential-level guidance establishing responsibilities of both geographic and functional combatant commanders (CCDRs), to include specific responsibilities for CWMD as well as other mission areas such as counterterrorism (CT), pandemic influenza and infectious disease (PI&ID), and homeland defense (HD). Various aspects of these responsibilities complement and overlap with the CWMD mission set.

III. DoD Strategy and Guidance

A. Defense Strategic Guidance

In January 2012, the Secretary of Defense (SecDef) released strategic guidance for DOD. Sustaining US Global Leadership: Priorities for 21st Century Defense reflects the President's strategic direction and recognizes that CWMD is one of ten primary missions of the US Armed Forces. This guidance emphasizes the threat posed by the proliferation of CBRN weapons technology to additional state actors and nonstate actors access to WMD. The guidance also recognizes that military forces conduct a range of activities to prevent the proliferation and use of WMD and states that, "in partnership with other elements of the USG, DOD will continue to invest in capabilities to detect, protect against, and respond to WMD use, should preventive measures fail."

B. Nuclear Posture Review

In April 2010, SecDef released the Nuclear Posture Review report, which described five objectives of nuclear weapons policies and posture: preventing nuclear proliferation and nuclear terrorism; reducing the role of US nuclear weapons in US NSS; maintaining strategic deterrence and stability at reduced nuclear force levels; strengthening regional deterrence and reassuring US allies and partners; and sustaining a safe, secure, and effective nuclear arsenal.

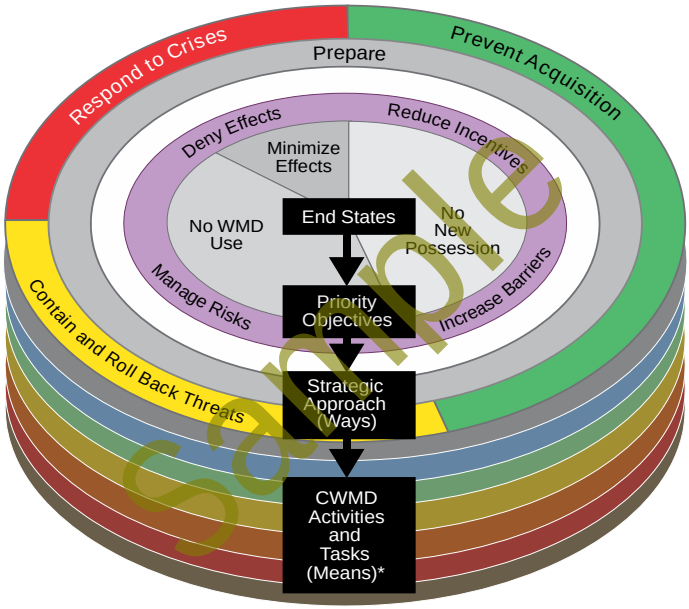
DODS-CWMD Strategic Approach

Ref: JP 3-40, Countering Weapons of Mass Destruction (Oct '14), pp. I-3 to I-4.

The objectives outlined in the DODS-CWMD are advanced through three CWMD lines of effort (LOEs): prevent acquisition, contain and reduce threats, and respond to crises. These three LOEs are supported by one strategic enabler; prepare. Together, the three LOEs and this strategic enabler comprise DOD's revised strategic approach for CWMD:

Strategy for Countering WMD

Department of Defense Strategy for Countering Weapons of Mass Destruction Strategic Approach



Ref: JP 3-40, Countering WMD, fig. I-1, p. I-4.

- **Prepare** is the continuous cycle that ensures DOD's set of enabling, foundational, and specialized activities, tasks, and capabilities support the CWMD LOEs
- **Prevent acquisition f**ocuses on actions to ensure that those not possessing WMD do not obtain them.
- **Contain and reduce threats** focuses on actions to reduce risks posed by extant WMD
- **Respond to crises** focuses on activities and operations to manage and resolve complex WMD crises

See following page for further discussion.

A. Nuclear and Radiological Weapons

Ref: JP 3-40, Countering Weapons of Mass Destruction (Oct '14), pp. II-1 to II-4.

Nuclear Weapons

Nuclear weapons derive their explosive power from the energy released during either fission or a combination of fission and fusion nuclear reactions. Fission is a process in which the nucleus of an atom splits into two or more nuclei and releases energy, fission products, and neutrons. The neutrons released by fission can, in turn, cause the fission of other fissile isotopes. Fissile material is composed of nuclides for which fission is possible with neutrons of any energy level. Fissile materials in a nuclear weapon—highly enriched uranium or plutonium—must achieve a supercritical state for a nuclear detonation to occur. Fusion is a process in which nuclei (generally light nuclei such as tritium and deuterium), combine and release energy, helium nuclei, and neutrons.

Single Stage Fission Weapons

- **Gun-assembled**. A gun-assembled device contains two or more pieces of fissile material, each a subcritical mass, brought together very rapidly to form a supercritical mass. A nuclear detonation results from a self-sustaining chain reaction of exponentially increasing numbers of fission events within that mass.
- **Implosion-assembled**. A spherical device in which a quantity of fission material normally at a density constituting a subcritical mass at ordinary pressure, can have its volume reduced suddenly by compression (a step typically accomplished by the use of chemical explosives) to form a supercritical mass at a much higher density. A nuclear detonation results from a supercritical chain reaction of exponentially increasing numbers of fission events within that mass.
- **Boosted Weapons**. A boosted weapon is an implosion-assembled weapon whose fission output is increased by thermonuclear neutrons from the fusion of deuterium and tritium gas introduced into the pit. This increases its explosive yield through fusion reactions that serve to increase the efficiency of the fission bomb.

Thermonuclear Weapons

A thermonuclear weapon is a device where radiation from a fission primary is used to transfer energy to compress and ignite a physically separate component containing thermonuclear fuel referred to as the secondary, resulting in nuclear fusion.

Improvised Nuclear Device

A device intended to produce a nuclear yield using fissile or fissionable material that is not developed and produced by a nation for military purposes. An improvised nuclear device may be fabricated from components developed by a state program or may be an improvised modification to a US or foreign weapon design.

Delivery Options

Nuclear weapons have been adapted for delivery by mortar, artillery shell, land mine, depth charge, torpedo, and missile. However, significant weapon design understanding is needed to produce a nuclear device that is both small enough and light enough to be delivered by such systems with reduced payload capacity. Given their significant destructive power, nuclear weapons need not be optimally employed to cause a mass casualty event. While nuclear weapons have been designed for stand-off delivery at specific altitudes and other conditions, they could simply be loaded onto a ship or truck, transported to the target, and detonated.

Nuclear Weapons Effects

When detonated, a nuclear weapon will release its energy as blast, thermal radiation, and nuclear radiation (alpha and beta particles, gamma rays, and neutrons). The interac-

Dirty Bombs (RDD)

Ref: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/fs-dirty-bombs.htm

A "dirty bomb" is one type of a radiological dispersal device (RDD) that combines conventional explosives, such as dynamite, with radioactive material. The terms dirty bomb and RDD are often used interchangeably in the media. Most RDDs would not release enough radiation to kill people or cause severe illness - the conventional explosive itself would be more harmful to individuals than the radioactive material. However, depending on the situation, an RDD explosion could create fear and panic, contaminate property, and require potentially costly cleanup. Making prompt, accurate information available to the public may prevent the panic sought by terrorists.

A dirty bomb is in no way similar to a nuclear weapon or nuclear bomb. A nuclear bomb creates an explosion that is millions of times more powerful than that of a dirty bomb. The cloud of radiation from a nuclear bomb could spread tens to hundreds of square miles, whereas a dirty bomb's radiation could be dispersed within a few blocks or miles of the explosion. A dirty bomb is not a "Weapon of Mass Destruction" but a "Weapon of Mass Disruption," where contamination and anxiety are the terrorists' major objectives.

Impact of a Dirty Bomb

The extent of local contamination would depend on a number of factors, including the size of the explosive, the amount and type of radioactive material used, the means of dispersal, and weather conditions. Those closest to the RDD would be the most likely to sustain injuries due to the explosion. As radioactive material spreads, it becomes less concentrated and less harmful. Prompt detection of the type of radioactive material used will greatly assist local authorities in advising the community on protective measures, such as sheltering in place, or quickly leaving the immediate area. Radiation can be readily detected with equipment already carried by many emergency responders. Subsequent decontamination of the affected area may involve considerable time and expense.

Immediate health effects from exposure to the low radiation levels expected from an RDD would likely be minimal. The effects of radiation exposure would be determined by:

- the amount of radiation absorbed by the body;
- the type of radiation (gamma, beta, or alpha);
- the distance from the radiation to an individual;
- the means of exposure-external or internal (absorbed by the skin, inhaled, or ingested); and the length of time exposed.
- The health effects of radiation tend to be directly proportional to radiation dose. In other words, the higher the radiation dose, the higher the risk of injury.

Protective Actions

In general, protection from radiation is afforded by:

- minimizing the time exposed to radioactive materials;
- maximizing the distance from the source of radiation; and
- shielding from external exposure and inhaling radioactive material.

Sources of Radioactive Material

Radioactive materials are routinely used at hospitals, research facilities, industrial activities, and construction sites. These radioactive materials are used for such purposes as diagnosing and treating illnesses, sterilizing equipment, and inspecting welding seams. The Nuclear Regulatory Commission together with 37 "Agreement" States, which also regulate radioactive material, administers more than 22,000 licenses of such materials. The vast majority of these materials are not useful as an RDD.

Application of Countering WMD Activity Construct

Ref: JP 3-40, Countering Weapons of Mass Destruction (Oct '14), fig. V-2, p. V-4.

Countering Weapons of Mass Destruction Lines of Effort		Notional Tasks Performed in Typical Operations and Missions	Countering Weapons of Mass Destruction Activity Categories			
			Understand the Environment	Cooperate with and Support Partners	Control, Defeat, Disable or Dispose of Weapons of Mass Destruction Threats	Safeguard the Force and Manage Consequences
	Prevent Acquisition		Locate, Identify, Characterize, Assess, Predict Intelligence, surveillance, and reconnaissance; medical planning and logistics	Partner, Coordinate Security cooperation; unified action; communication synchronization; interdiction; target planning; civil-military cooperation; border security	Divert and Intercept, Seize, Delay or Disrupt, Neutralize, and Destroy Targeting; interdiction; information operations; ntelligence, surveillance, and reconnaissance; communication synchronization	Mitigate and Sustain Force protection
	Contain, Reduce Threats		Locate, Identify, Characterize, Assess, Predict Intelligence, surveillance, and reconnaissance; weapons technical intelligence; medical planning and logistics; meteorological and oceanographic operations	Partner, Coordinate Security cooperation; unified action; bio-surveillance; strategic communications; targeting; information operations	Divert and Intercept, Isolate, Secure, Seize, Delay or Disrupt, Neutralize, Destroy, Exploit, Degrade, Reduce, Dismantle, Redirect, and Monitor Targeting; interdiction; site security; site exploitation; special forces and unified action; cooperative threat reduction; cooperation; civil-military cooperation; sanctions enforcement	Mitigate, Sustain, Support Force protection; health services; route reconnaissance
	Respond to Crises		Locate, Identify, Characterize, Assess, Attribute, and Predict Intelligence, surveillance, and reconnaissance; force posturing; bio-surveillance; forensics and evidence collection; hazard modeling	Partner, Coordinate Security cooperation; unified action; civil-military cooperation; communication synchronization; force protection; logistics	Divert and Intercept, Isolate, Secure, Seize, Delay or Disrupt, Neutralize, Destroy, Exploit, Degrade, Mitigate, Sustain, Support Targeting; interdiction; site security; information operations; special forces and unified action; force protection	Mitigate, Sustain, Support Force protection; health services; decontamination operations; contamination avoidance

Understand the Environment, Threats, and Vulnerabilities

Ref: JP 3-40, Countering Weapons of Mass Destruction (Oct '14), pp. V-5 to V-6.

1. Locate Task

The JFC uses SOF, and intelligence collection assets to locate WMD-associated system nodes and program elements, to include production facilities, storage/stockpile sites, and key program personnel. Developing robust information sharing relationships with interorganizational partners, particularly related to identity data, is an essential component to this task.

2. Identify Task

Once a WMD-related element and capability is located, the JFC's intelligence staff, in coordination with interorganizational experts, scope, categorize, and prioritize the posed threat. Confirmation of a threat will lead to further analysis to characterize and then assess specific elements of the program more effectively. During conflict, initial identification of CBRN materials will most likely be performed by conventional forces.

3. Characterize Task

Prior to conflict, the JFC gains understanding of an actor of concern's WMD program by mapping its individual components, its internal linkages, and its external associations through a variety of intelligence collection and analysis capabilities. This includes the types of weapons and the related materials, technology, and expertise associated with each WMD capability. The JFC staff uses characterization to inform assessment, attribution, and predictive analysis. During and after conflict, characterization occurs when the joint force has access to and can fully examine WMD facilities, stockpiles, weapons, and/or personnel.

4. Assess Task

Analysis conducted in conjunction with larger DOD, civilian, USG, and international partners interorganizational effort helps the JFC determine the threat posed by an actor of concern's WMD program. This includes an assessment by the JFC staff of US and PN vulnerabilities in relation to a specific actor's WMD capability. The JFC may use hazard estimation, measurement, and modeling systems, as well as multinational exercises to assess the level of threat that an actor of concern's WMD poses to US and friendly forces.

5. Attribute Task

Attribution is an effort to determine the origin of the material or weapon as well as those responsible for a CBRN event. The process derives forensics conclusions from the definitive analysis of samples collected, law enforcement, and intelligence information. Forensic-enabled intelligence collection, processing, exploitation, and analysis capabilities support the identification of CBRN sourcing and attribution. Joint forces directly support the attribution process through intelligence (e.g., site exploitation), sample collection and transfer, and technical analysis. These forces require training, certification, and specialized equipment and expertise, and in some cases, unique authorities that must be requested by the JFC prior to execution. These forces must be identified early in the planning process.

6. Predict Task

Specialized, technical capabilities are used to construct a common operational picture presenting current and forecasted information on the actors of concern, friendly forces, neutral elements, the environment, and geospatial information. JFCs use modeling, diagnostics, intelligence, and analysis capabilities to understand the current environment, detecting anomalies, and continually assessing the WMD threat and related networks to extrapolate possible future threats.

B. CWMD Activity 2: Cooperate with and Support Partners

This activity promotes common threat awareness, builds CWMD self-sufficiency, improves military interoperability, enhances military and civilian preparedness, deterrence, and in some cases facilitates security of dual-use and CBRN materials. JFCs should plan to perform tasks associated with this activity in full cooperation with state and local authorities, USG interagency partners in a variety of departments and agencies, multinational partners, and NGOs. The JFC will coordinate with state and local authorities, interagency partners, multinational partners, and NGOs to ensure the partner and coordinate tasks associated with this activity are successfully conducted, to various degrees, within military engagement, SC, CTR, and deterrence operations and activities during all military operational phases. The JFC should seek to strengthen existing partner relationships and support programs to build the foundation for future partnering opportunities. Whenever conducting this activity, CCMDs coordinate with DOS to make contact with international counterparts in PNs. JFCs need to include partners in planning and execution processes as early as possible. GCCs can then leverage existing activities, such as interorganizational and multinational training and exercises to strengthen relationships and improve regional capabilities and capacity to achieve CWMD objectives. As part of this activity, CCMDs should coordinate with DOS to make contact with international counterparts.

Partner Task

Domestic and foreign security partnerships support the collective capability to respond to and defeat WMD threats and manage the consequences of an attack. Existing partnerships must be maintained and new relationships sought out, building partner capacity in key areas that support deterrence and all operational phases.

Coordinate Task

Promote and improve common threat awareness, interoperability, response preparedness, and WMD risk reduction. Actions that support this task include operational planning with partners and SC efforts that synchronize counterproliferation activities such as interception.

C. CWMD Activity 3: Control, Defeat, Disable, and/or Dispose of WMD Threats

The purpose of the control, defeat, disable, and/or dispose of WMD threats activity is to reduce WMD-related threats. DOD has developed specialized capabilities and units to address the tasks associated with this CWMD activity. When conducted on a small scale, this activity may constitute part or all of a crisis response or limited contingency operation. For major operations and campaigns, which balance offensive, defensive, and stability operations, this activity supports the joint force's offensive actions. Typically, JFCs control, defeat, disable, or dispose of individual WMD threats, as appropriate. These tasks may be conducted utilizing lethal and/or nonlethal capabilities that require specialized equipment and expertise. The JFC should focus on controlling an actor of concern's program elements and then transitioning control to a competent authority for final disposition as the situation/mission dictates.

See following pages (pp. 7-36 to 7-37) for an overview and further discussion.

Chap 8

Consequence Management (CM)

Ref: JP 3-41, Chemical, Biological, Radiological, and Nuclear Consequence Management (Jun '12), chap. 1 and ATP 3-11.41, Multi-Service TTPs for CBRN Consequence Management Operations (Jul '15).

This chapter overviews response to disasters – both natural and man-made, and addresses issues related to consequence management of natural disasters or acts of terrorism, including weapons of mass destruction (WMD) events. Responding to terrorism involves instruments that provide crisis management and consequence management.

(Sgt. Melissa Parrish / U.S. Army)

Crisis Management

"Crisis management" refers to measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. The Federal Government exercises primary authority to prevent, preempt, and terminate threats or acts of terrorism and to apprehend and prosecute the perpetrators; State and local governments provide assistance as required. Crisis management is predominantly a law enforcement response.

Consequence Management

"Consequence management" refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise primary authority to respond to the consequences of terrorism; the Federal Government provides assistance as required. Consequence management is generally a multifunction response coordinated by emergency management.

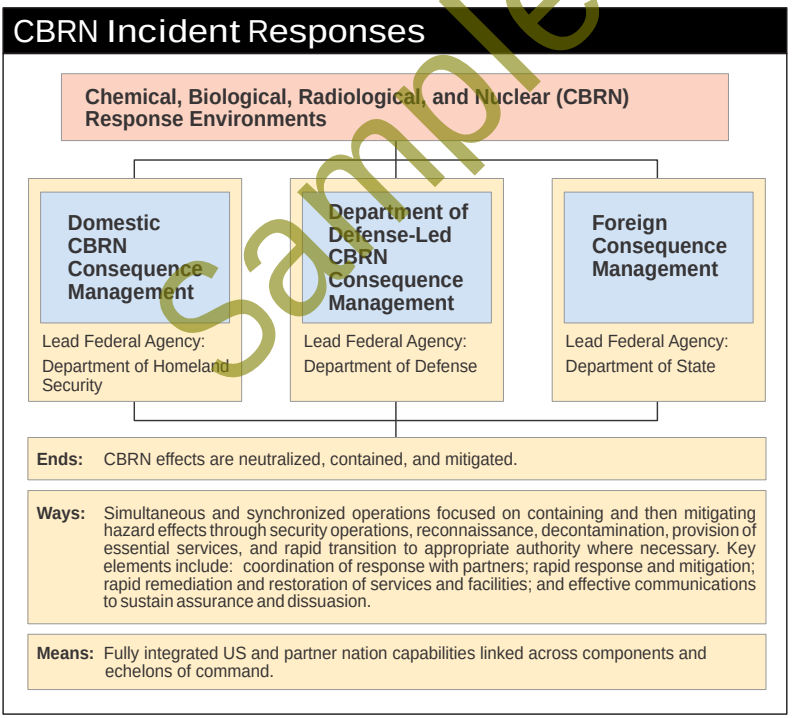
This chapter provides information on the National Response Framework (NRF) aligns federal coordination structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management. It includes

and understanding of how local, state, and federal emergency agencies interact and discusses how to plan and construct consequence and contingency plans to meet both natural and man-made emergencies.

The National Incident Management System (NIMS) is a comprehensive approach to all aspects of incident management, regardless of size, complexity, or cause. The guidance for NIMS was published by the Department of Homeland Security (DHS) in March 2004, and the guidance continues to be refined and updated by the NIMS Integration Center. One of the six primary elements of NIMS is the use of a standardized command and management system for incident scene operations, the Incident Command System (ICS); and for supporting operations centers, the Multiagency Coordination System.

I. United States Government (US) Approach to a CBRN Incident

The USG approach to managing the consequences of a CBRN incident is vested in chemical, biological, radiological, and nuclear consequence management (CBRN CM). CBRN CM can be described as the overarching USG capability and the strategic national direction, to prepare for, respond to, and recover from the effects of a CBRN incident at home or abroad, and whether or not it is attributed to an attack using weapons of mass destruction (WMD). When required, the USG will coordinate its response to a CBRN incident in one of three ways based on the geopolitical situation.



Ref: JP 3-41, CBRN Consequence Management, fig. I-1, p. I-3.

The Department of Homeland Security (DHS) is the USG lead agency for incident management that would include a domestic CBRN incident. Overseas, excluding homeland areas, the Department of State (DOS) is the USG lead for what is termed

I. All Hazards Response

Ref: JP 3-28, Defense Support of Civil Authorities (Jul '14), chap. 2.

I. The Nature of a Catastrophic Incident

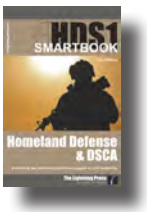
A catastrophic incident, as defined by the NRF, is "any natural or man-made incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions." Catastrophic incident is the same as catastrophic event as defined by DOD. A catastrophic event could result in significant nationwide impacts over a prolonged period of time. It almost immediately exceeds resources normally available to state, territory, tribal, local, and private-sector authorities in the impacted area, and it significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.

> ***Complex Catastrophe***
>
> *Any natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple, interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions.*
>
> *Deputy Secretary of Defense Memorandum, 19 February 2013*

The catastrophic event becomes complex (complex catastrophe) when it causes cascading failures of multiple, interdependent, critical life-sustaining infrastructure, in which disruption of one infrastructure component (such as the electric power grid) disrupts other infrastructure components (such as transportation and communications).

Recognizing that federal or national resources are required to augment overwhelmed state, interstate, territory, tribal, and local response efforts, the NRF—Catastrophic Incident Annex establishes protocols to pre-identify and rapidly deploy key essential resources (e.g., medical teams, search and rescue [SAR] teams, transportable shelters, medical and equipment caches, and emergency communications) required to save lives and contain incidents.

When a situation is beyond the capability of an affected state or territory, the governor may request federal assistance from the President. The President may also proactively direct the federal government to provide supplemental assistance to state, territorial, tribal, and local governments to alleviate the suffering and damage resulting from disasters or emergencies.



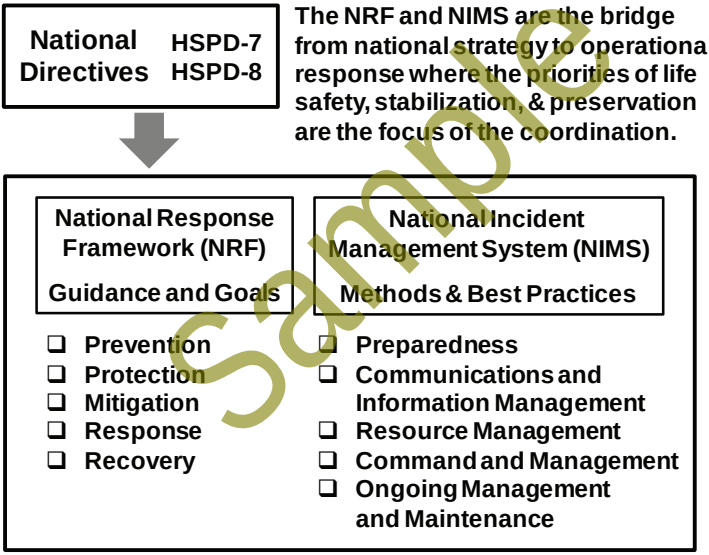
Refer to The Homeland Defense & DSCA SMARTbook (Protecting the Homeland / Defense Support to Civil Authority) for further discussion. Topics and references include homeland defense (JP 3-28), defense support of civil authorities (JP 3-28), Army support of civil authorities (ADRP 3-28), multi-service DSCA TTPs (ATP 3-28.1/MCWP 3-36.2), DSCA liaison officer toolkit (GTA 90-01-020), key legal and policy documents, and specific hazard and planning guidance.

II. National Incident Management System (NIMS) & the National Response Framework (NRF)

The NRF and NIMS are two parts of a combined effort with the NRF providing the framework for the goals of response and NIMS providing the active development of systems to meet these goals within standardized response efforts. The goals and the systems are interlocked and one program is not "over" the other.

The National Response Framework (NRF) is a guide to how the Nation conducts all-hazards response. It builds upon the NIMS coordinating structures to align key roles and responsibilities across the Nation, linking all levels of government, nongovernmental organizations, and the private sector.

The National Incident Management System (NIMS) provides the incident management basis for the National Response Framework (NRF) and defines standard command and management structures. Standardizing national response doctrine on NIMS provides a consistent, nationwide template to enable the whole community to work together to prevent, protect against, mitigate, respond to, and recover from the effects of incidents regardless of cause, size, location, or complexity.



National Directives, Laws, and Presidential Orders provide the strategic goals of national response and frame concepts like preservation of our way of government and what essential services and functions the government must perform in order to provide the people with the requirements of governance: security, essential services, Rule of Law, and economic opportunity. These things are provided by government in order to maintain an environment of stability within the social construct the nation. These goals are strategic. Response to disaster is a subset of this greater design for stability.

The function of the NRF and NIMS is to take those strategic concepts and convert them from strategic national goals to a standardized system of operational response methodologies that can be used at the state and local level. This is still a wide scope and the methods described are general application and can be used in most situations. This is call an All Hazards approach.

Emergency Support Functions (ESFs)

Ref: ATP 3-28.1, Multi-Service TTP for DSCA (Feb '13), table 1, pp. 4-5 .

Emergency Support Functions (ESFs)

ESFs	Coordinator
#1 Transportation	Department of Transportation
#2 Communications	Department of Homeland Security (DHS) – National Communications System
#3 Public Works and Engineering	Department of Defense (DOD) – US Army Corps of Engineers
#4 Firefighting	United States Department of Agriculture (USDA) – US Forest Service
#5 Emergency Management	DHS – Federal Emergency Management Agency(FEMA)
#6. Mass Care, Emergency Assistance, Housing, and Human Services	DHS – FEMA
#7 Logistics Management and Resource Support	General Services Administration and DHS – FEMA
#8 Public Health and Medical Services	Department of Health and Human Services
#9 Search and Rescue	DHS – FEMA
#10 Oil and Hazardous Materials Response	Environmental Protection Agency
#11 Agriculture and Natural Resources	USDA
#12 Energy	Department of Energy
#13 Public Safety and Security	Department of Justice
#14 Long-Term Community Recovery	DHS – FEMA
#15 External Affairs	DHS

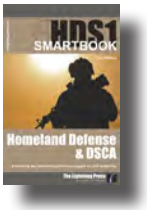
Note: DOD is a supporting agency for all ESFs except ESF #3, Public Works and Engineering. Although the Army Corps of Engineers is the Coordinator for #3, it does so based upon its congressionally mandated status and not as a subordinate part of a federal military joint task force.

Refer to Disaster-Response SMARTbook 2 – Incident Command System (ICS) (On-Scene, All-Hazards Incident Management) for further discussion. Topics include incident command system (ICS) purpose, features, and principles; command and staff functions; leadership and management; unified command, area command, and multiagency coordination; planning; ICS briefings and meetings; organizational flexibility; incident/event management; resource management; and demobilization.

- Readiness (impact on DOD's ability to perform its primary mission)

DSCA plans will be compatible with the NRF, NIMS, and DOD issuances. DSCA planning will consider C2 options that emphasize unity of effort.

With limited exceptions (e.g., local requests for immediate and emergency response), initial RFAs will be directed to the OSD, Executive Secretariat. SecDef-approved RFAs are assigned to the appropriate CCDR. The supported CCDR determines the appropriate level of C2 for each response and usually directs a senior military officer to deploy to the incident site. However, in the USPACOM AOR, CDRUSPACOM has delegated this responsibility to Commander, Joint Task Force (CJTF)-Homeland Defense. The DCO serves as DOD's single point of contact in the JFO. Requests will be coordinated and processed through the DCO with the exception of requests for United States Army Corps of Engineers (USACE) support, NG forces operating in state active duty or Title 32, USC, status (i.e., not in federal service), or, in some circumstances, DOD forces in support of the Federal Bureau of Investigation (FBI) or the United States Secret Service (USSS).

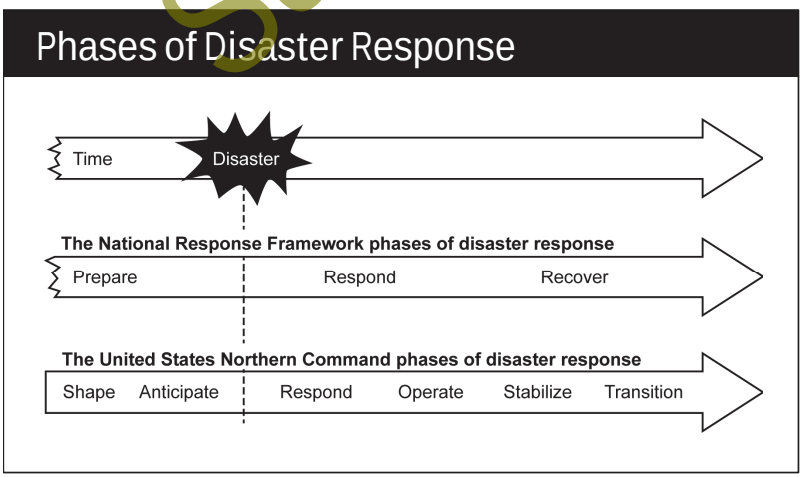


Refer to The Homeland Defense & DSCA SMARTbook (Protecting the Homeland / Defense Support to Civil Authority) for further discussion. Topics and references include homeland defense (JP 3-28), defense support of civil authorities (JP 3-28), Army support of civil authorities (ADRP 3-28), multi-service DSCA TTPs (ATP 3-28.1/MCWP 3-36.2), DSCA liaison officer toolkit (GTA 90-01-020), key legal and policy documents, and specific hazard and planning guidance.

IX. Phases of Disaster Response

(ADRP 3-28) Commanders conducting DSCA planning should be familiar with the phases of disaster response operations, as used in the NRF and in USNORTHCOM plans for DSCA. USNORTHCOM planners use six operational phases, which are similar to the flexible phasing model described in JP 3-0 but somewhat modified for DSCA: shape, anticipate, respond, operate, stabilize, and transition. The NRF uses three phases: prepare, respond, and recover. The figure below illustrates the relationship between the NRF phases and the USNORTHCOM phases.

Army doctrine does not specify operational phases. Refer to ADRP 3-0, chapter 2.



Ref: ADRP 3-28 DSCA, fig. 1-10, p. 1-29.

See following page for further discussion of the five operational phases.

Operation Phases of Defense Support of Civil Authorities

Ref: JP 3-28, Defense Support of Civil Authorities (Jul '14), p. II-15 to II-16.

DSCA operations are generally conducted in six phases: shape, anticipate, respond, operate, stabilize, and transition. During planning, the JFC establishes conditions, objectives, or events for transitioning from one phase to another. Phases are designed to be conducted sequentially, but some activities from a phase may begin in a previous phase and continue into subsequent phases. A DSCA operation may be conducted in multiple phases simultaneously if the JOA has widely varying conditions.

Phase 0 (Shape)

Phase 0 is continuous situational awareness and preparedness. Actions in this phase include interagency coordination, planning, identification of gaps, exercises, and public affairs (PA) outreach. These activities continue through all phases. Shaping operations are inclusive of normal and routine military activities and various interagency activities to assure or solidify relationships with partners, friends, and allies. This phase sets the conditions for expanded interoperability and cooperation with interagency partners via active engagements in planning, conferences, training programs and exercises, and coordination and interaction.

Phase I (Anticipate)

Phase I begins with the identification of a potential DSCA mission, a no-notice event, or when directed by the President or SecDef. The phase ends with assigned response forces deployed or when the determination is made that there is no event requiring DSCA response. Phase I success is achieved when deployment of a DCO, EPLO, and other selected response forces is accomplished. These forces are postured to facilitate quick response after coordination with the primary agency PFO/JFO and coordination with state, local, and tribal officials.

Phase II (Respond)

Phase II begins with the deployment of initial response capabilities. The phase ends when response forces are ready to conduct operations in the JOA. Phase II success is achieved when forces are deployed with sufficient capability to support civil authorities in accomplishment of the mission. DSCA operations are based on RFAs, which will be made at different times, and for missions that will be completed at different times. Consequently, forces will likely deploy into and out of the JOA during the entire DSCA operation.

Phase III (Operate)

Phase III begins when DSCA response operations commence. Phase III ends when Title 10, USC, forces begin to complete mission assignments and no further requests for DOD assistance are anticipated from civil authorities. Phase III success is achieved when currently deployed DOD capabilities are sufficient to support civil authorities.

Phase IV (Stabilize)

Phase IV begins when military and civil authorities decide that DOD support will scale down. Phase IV ends when DOD support is no longer required by civil authorities and transition criteria are established. Phase IV success is achieved when all operational aspects of mission assignments are complete.

Phase V (Transition)

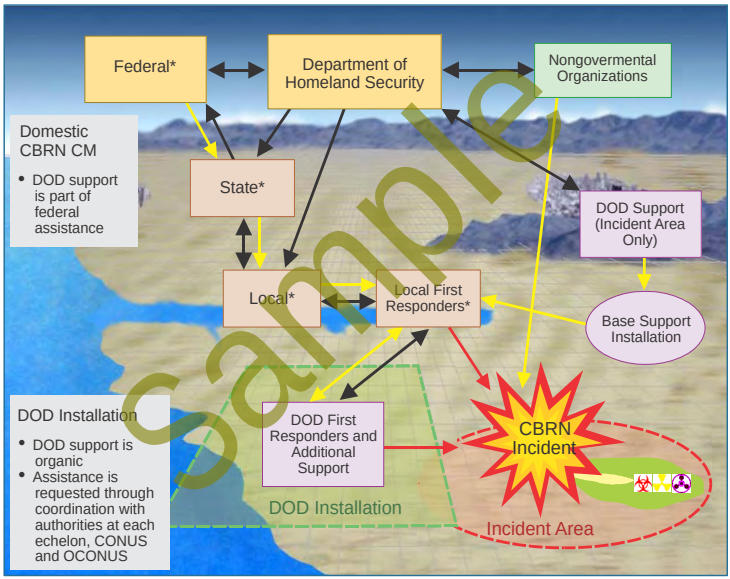
Phase V begins with the redeployment of remaining DOD forces. The phase ends when response forces have been relieved, redeployed, and OPCON is transferred to their respective commands. Phase V success is achieved when DOD forces have transitioned all operations back to civil authorities.

III. Domestic Consequence Management (CM)

Ref: JP 3-41, Chemical, Biological, Radiological, and Nuclear Consequence Management (Jun '12), chap. 2.

CBRN CM conducted by DOD in the homeland in support of civil authorities is conducted as a DSCA operation. The capability and capacity to effectively respond to domestic CBRN incidents and sustain operations in CBRN environments require properly trained and equipped forces that follow the parameters set forth in this section.

Domestic CBRN Consequence Management



*Tribal response may require special consideration during coordination.

Legend

CBRN	chemical, biological, radiological, and nuclear
CBRN CM	chemical, biological, radiological, and nuclear consequence management
CONUS	continental United States
DOD	Department of Defense
OCONUS	outside the continental United States

request for assistance/coordination
provision of assistance
response to incident

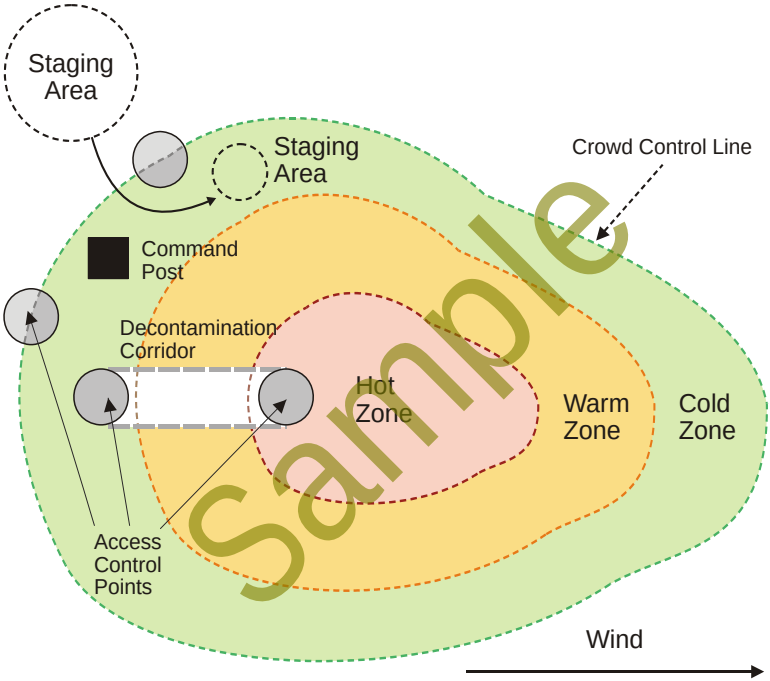
Ref: JP 3-41, CBRN Consequence Management, fig. II-1, p. II-2.

A description of DOD's participation in the whole-of-government response to a domestic CBRN incident is provided in the NRF. It further details the authorities that delineate the roles and limits for DOD in a domestic response. In conducting DSCA to include CBRN response, a distinction is made between the different chains of command for active DOD, Title 10, USC, federal forces providing support to civil authorities and for NG forces commanded by the state governor under Title 32, USC,

VI. CBRN Control Zones

Ref: JP 3-41, Chemical, Biological, Radiological, and Nuclear Consequence Management (Jun '12), pp. II-29 to II-31 (fig. II-5, p. II-30).

In CBRN response, control zones are established to ensure the safety of all responders and control access into and out of a contaminated area. The three zones established at a chemical, radiological, nuclear, and some biological incident sites (where there is a contaminated area such as may be the case with anthrax) are often referred to as the hot zone, the warm zone, and the cold zone. Figure II-5 depicts these control zones. In nearly all cases, the control zones will decrease in size with time as CBRN hazards naturally decrease. Once the characteristics of the hazard are understood, the control zones can be effectively altered to allow more mission flexibility.



1. Hot Zone

The hot zone is an area immediately surrounding a hazardous material incident which extends far enough to prevent adverse effects from released contamination to personnel outside the zone. The level of risk and thus the included area is determined by the incident commander, accounting for characteristics of the hazards. The hot zone can also be referred to as the exclusion zone, red zone, or restricted zone and is the primary area of contamination. The hot zone is the area that the incident commander judges to be the most affected by the incident. This includes any area to which the contaminant has spread or is likely to spread. Primary contamination can occur when individuals enter this zone. Usually, no decontamination or patient care except evacuation is carried out in this zone. Access is only permitted to personnel who are properly trained and protected. The incident commander sets the perimeters of this zone after giving consideration to the

(CTS1) Index

D

E

F

G

H

R

S

T

U

V

W

SMARTbooks

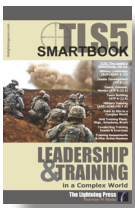
INTELLECTUAL FUEL FOR THE MILITARY

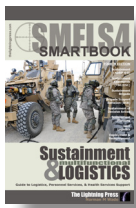
MILITARY REFERENCE: JOINT & SERVICE-LEVEL

Recognized as a "whole of government" doctrinal reference standard by military professionals around the world, SMARTbooks comprise a comprehensive professional library.

MILITARY REFERENCE: MULTI-SERVICE & SPECIALTY

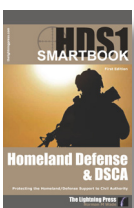
SMARTbooks can be used as quick reference guides during operations, as study guides at professional development courses, and as checklists in support of training.





HOMELAND DEFENSE, DSCA, & DISASTER RESPONSE

Disaster can strike anytime, anywhere. It takes many forms—a hurricane, an earthquake, a tornado, a flood, a fire, a hazardous spill, or an act of terrorism.

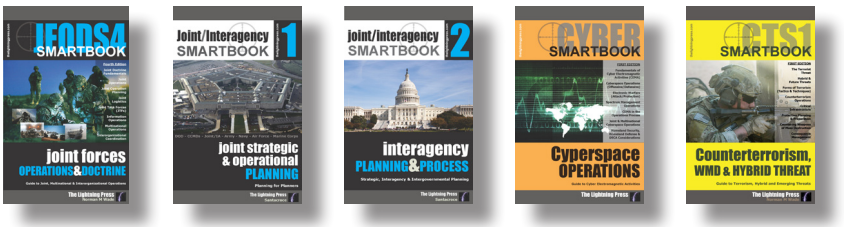


The Lightning Press is a **service-disabled, veteran-owned small business,** DOD-approved vendor and federally registered — to include the SAM, WAWF, FBO, and FEDPAY.

RECOGNIZED AS THE DOCTRINAL REFERENCE STANDARD BY MILITARY PROFESSIONALS AROUND THE WORLD.

JOINT STRATEGIC, INTERAGENCY, & NATIONAL SECURITY

The 21st century presents a global environment characterized by regional instability, failed states, weapons proliferation, global terrorism and unconventional threats.



THREAT, OPFOR, REGIONAL & CULTURAL

In today's complicated and uncertain world, the military must be ready to meet the challenges of any type of conflict, in all kinds of places, and against all kinds of threats.

DIGITAL SMARTBOOKS (eBooks)

Our eBooks are a true "A–B" solution! Solution A is that our digital SMARTbooks are available and authorized to a user's Adobe ID and can be transferred to up to six computers and devices via Adobe Digital Editions, with free software available for **85+ devices and platforms—including PC and MAC, iPad, Android Tablets and Phones, and more.** Solution B is that you can also use our digital SMARTbooks through our dedicated SMARTbooks iPad App!

View, download FREE samples and purchase online:

www.TheLightningPress.com

Purchase/Order

www.TheLightningPress.com

SMARTsavings on SMARTbooks! Save big when you order our titles together in a SMARTset bundle. It's the most popular & least expensive way to buy, and a great way to build your professional library. If you need a quote or have special requests, please contact us by one of the methods below!

View, download FREE samples and purchase online:

www.TheLightningPress.com

Order SECURE Online

Web: www.TheLightningPress.com

Email: SMARTbooks@TheLightningPress.com

Phone Orders, Customer Service & Quotes

Live customer service and phone orders available Mon - Fri 0900-1800 EST at (863) 409-8084

24-hour Voicemail/Fax/Order

Record or fax your order (or request a call back) by voicemail at 1-800-997-8827

Mail, Check & Money Order

2227 Arrowhead Blvd., Lakeland, FL 33813

Government/Unit/Bulk Sales

The Lightning Press is a **service-disabled, veteran-owned small business**, DOD-approved vendor and federally registered—to include the SAM, WAWF, FBO, and FEDPAY.

We accept and process both **Government Purchase Cards** (GCPC/GPC) and **Purchase Orders** (PO/PR&Cs).

*The Lightning Press offers design, composition, printing and production services for units, schools and organizations wishing their own **tactical SOP, handbooks, and other doctrinal support materials**. We can start a project from scratch, or our SMARTbooks can be edited, custom-tailored and reproduced with unit-specific material for any unit, school or organization.*

VISA MasterCard American Express Cards PayPal

CTS1

thelightningpress.com

Counterterrorism, WMD & Hybrid Threat SMARTBOOK

Guide to Terrorism, Hybrid and Emerging Threats

Terrorism has evolved as a preferred tactic for ideological extremists around the world, directly or indirectly affecting millions of people. Terrorists use many forms of unlawful violence or threats of violence to instill fear and coerce governments or societies to further a variety of political, social, criminal, economic, and religious ideologies.

A **hybrid threat** is the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually-benefiting effects.

Counterterrorism activities and operations are taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals.

Weapons of mass destruction (WMD) are chemical, biological, radiological, or nuclear (CBRN) weapons or devices capable of a high order of destruction and/or causing mass casualties.

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy - the infrastructure. **Protection** is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area.

Consequence management refers to measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.

DIME is our DOMAIN!™

SMARTbooks: Reference Essentials for the Instruments of National Power

Part of our "Military Reference" Series

ISBN 9781935886433
90000 >
9 781935 886433

www.TheLightningPress.com