NCTC and Information Sharing

FIVE YEARS SINCE 9/11: A PROGRESS REPORT

SEPTEMBER 2006

NCTC AND INFORMATION SHARING
FIVE YEARS SINCE 9/11: A PROGRESS REPORT

The performance of the United States Government in the years leading up to the terrorist attacks on September 11, 2001 was hindered by inadequate information sharing between key agencies of the Federal government.

> "Managers should have ensured that information was shared and duties were clearly assigned across agencies, and across the foreign domestic divide."
>
> —*9/11 Commission Report*

> "Prior to September 11th, there was a failure to share terrorism-related information rapidly and efficiently within agencies; among entities within the Intelligence Community tasked with producing intelligence to support counterterrorism efforts; and with state, local, and tribal law enforcement."
>
> – *WMD Commission Report*

The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 assigned to the National Counterterrorism Center (NCTC) the responsibility "to ensure the agencies, as appropriate, have access to and receive all-source intelligence products needed to execute their counterterrorism plans or perform independent, alternative analysis," and "to ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities." NCTC statutory authorities are limited to sharing with Federal organizations.

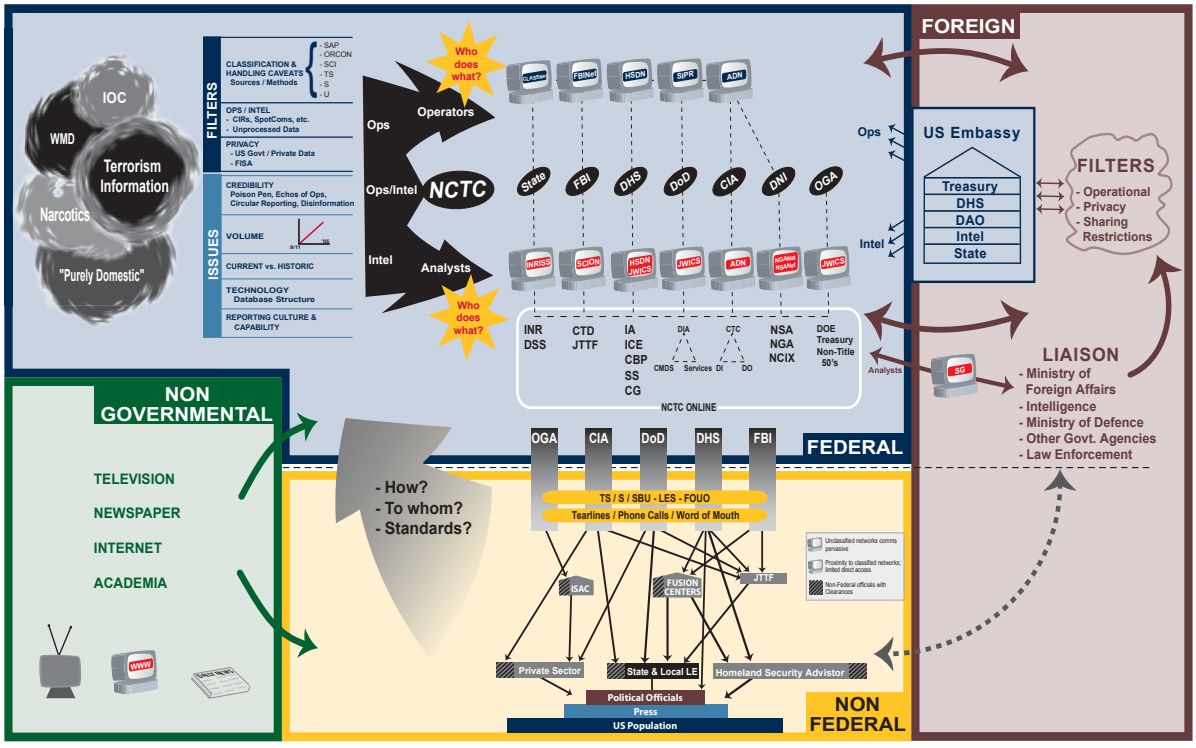
This report focuses on the progress that NCTC, working with its Federal partners, has made in the years since 9/11. It does not address the many efforts by other departments and agencies to improve information sharing at the Federal level and with non-Federal partners.

COMPLEXITY

Information sharing in support of the nation's counterterrorism objectives isn't about "flipping a switch;" it involves a diverse landscape of players and technologies, and myriad cultural, security, and policy barriers. Specific challenges include:

- Recognizing and designating "terrorism" information.
- Protecting operationally sensitive information.
- Ensuring that constitutional rights of individuals are not violated through information sharing practices.
- Clarifying roles, responsibilities, and information needs of the members of the counterterrorism community.
- Developing a considered approach to information sharing across Federal, state, and local levels amidst ever-increasing numbers of networks and databases.

The complexity of the information sharing challenge as it has existed for the last several years can be seen below.



The Complexities of Information Sharing

INFORMATION INTEGRATION

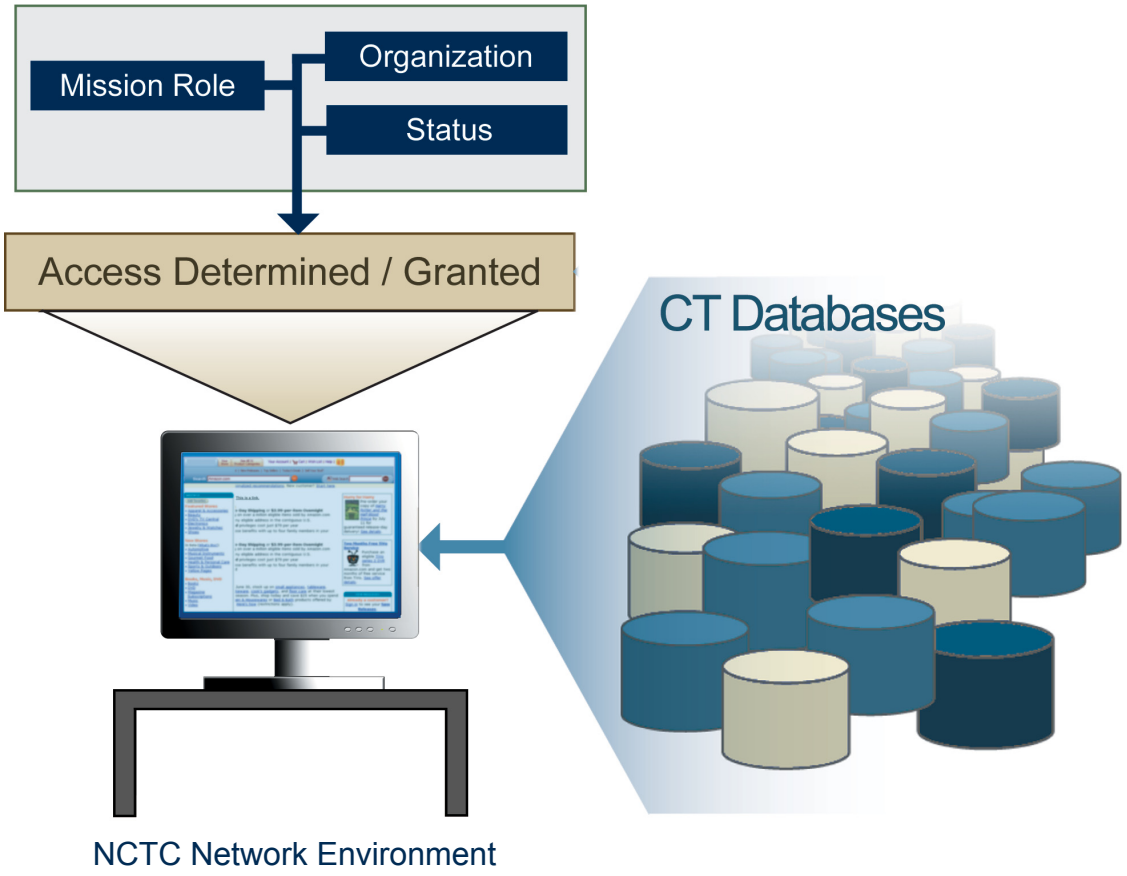
PRIOR TO 9/11

No organization in the US Government had access to the full range of terrorism information available to the various Federal agencies and departments.

TODAY

Analysts at NCTC have access to dozens of networks and information systems from across the intelligence, law enforcement, military, and homeland security communities, containing many hundreds of data repositories. These systems contain foreign and domestic information pertaining to international terrorism and sensitive operational and law enforcement activities. NCTC is exploring capabilities to help analysts integrate and assimilate this enormous volume of terrorism-related information.

A role-based access philosophy has been adopted to accommodate legal and collector concerns that not all individuals should have access to particularly sensitive information.



SITUATIONAL AWARENESS

PRIOR TO 9/11

There was no systematic means of maintaining routine situational awareness regarding the terrorist threat either across the US Government or with foreign partners.

TODAY

NCTC hosts counterterrorism community-wide secure video teleconferences (SVTCs) three times daily to ensure broad awareness of ongoing operations and newly detected threats. During these SVTCs, participants compare notes, highlight new threats, and debunk erroneous reports.

The NCTC Operations Center, collocated with its CIA and FBI counterparts, works with eleven other counterterrorism community operations centers on a daily basis and up to thirty-four more as events demand.

NCTC provides input to the *Presidents Daily Brief*, and produces daily the *National Terrorism Bulletin, Senior Executive Threat Report*, *Threat Matrix*, terrorism situations reports (twice daily), numerous special analysis reports, spot commentaries, threat alerts, advisories, and assessments summarizing the latest intelligence reporting related to terrorism threats.

NCTC provides coordinated counterterrorism community support to national security events, such as the 2004 Olympics, both national Presidential Conventions, and the Presidential Inauguration.

NCTC maintains the US Government database on worldwide terrorist incidents. This unclassified database is available at www. nctc.gov for the benefit of all interested in terrorism.

NCTC Operation Center

ENABLING ALL ELEMENTS OF STATE POWER

PRIOR TO 9/11

The US Government could not bring all elements of state power to bear against the terrorism threat, in part because departments and agencies lacked a common frame of reference. There was no widely available classified electronic library of terrorism information, and classified intelligence dissemination practices did not adequately support the range of US Government organizations involved in counterterrorism activities.

TODAY

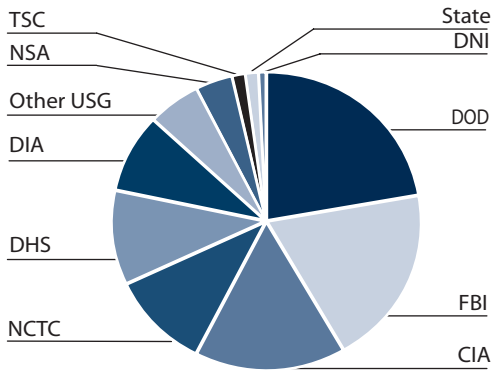
NCTC hosts a classified repository, NCTC Online (NOL), that serves as the counterterrorism community's library of terrorism information. This repository reaches the full range of intelligence, law enforcement, military, homeland security, and other Federal organizations involved in the global war on terrorism. The creation of NOL, coupled with policy changes, has allowed nonintelligence community agencies easier access to counterterrorism information, and has resulted in broad and robust sharing of intelligence information.

Sample NCTC Online Homepage

Today NOL hosts:

- Over 6,000 users.
- 6 million documents.
- Over 60 contributing departments and agencies.

NOL User Groups



OTHER USG	DOD
Agriculture	Air Force
Bureau of Alcohol, Tobacco & Firearms	Air Force Office of Special Investigations
Capitol Police	Army
Commerce	Joint Chiefs of Staff
Energy	Counterintelligence Field Activities
Federal Aviation Administration	Joint Warfare Analysis Center
Federal Reserve Board	Marines
Health & Human Services	National Ground Intelligence Center
Interior	National Geospatial-Intelligence Agency
Justice	Naval Surface Warfare Development Group
National Recon Office	Navy
National Security Council	All Major Commands
Nuclear Regulatory Commission	
Transportation	
Treasury	

BUSINESS PROCESS AND PARTNERSHIPS

PRIOR TO 9/11

Roles and responsibilities within the counterterrorism community were poorly defined and redundant; information sharing was limited, analysis and production were not coordinated, and dissemination was departmentally focused.

TODAY

Federal counterterrorism roles and responsibilities are being coordinated across the US Government.

The counterterrorism community Production Planning Board, consisting of representatives from CIA, FBI, DHS, DIA, NSA, NGA, and others, meets daily to plan and coordinate analytic efforts and ensure that all issues receive appropriate resources.

The Interagency Intelligence Committee on Terrorism (IICT) now comprises more than 100 members, meets monthly at NCTC, and actively coordinates critical counterterrorism issues such as emerging threats and threat countermeasures.

Information flow and dissemination have been improved through standardization of the format and use of tearlines, and the elimination of cold-war era rules that restricted the flow of intelligence among departments and agencies of the US Government.

Congress established a Program Manager for the Information Sharing Environment (PM ISE) tasked to improve terrorism information sharing among Federal and non-Federal entities. Federal agencies, in cooperation with the PM ISE are working to integrate business processes to ensure reliable information flow among Federal, state, local, tribal and private sector entities. NCTC works closely with the PM ISE as an active member of the Information Sharing Council.

NCTC has an active foreign liaison role engaging counterparts, providing sanitized versions of counterterrorism products, hosting conferences, and forward-deploying NCTC officers as warranted.

TERRORIST IDENTITIES

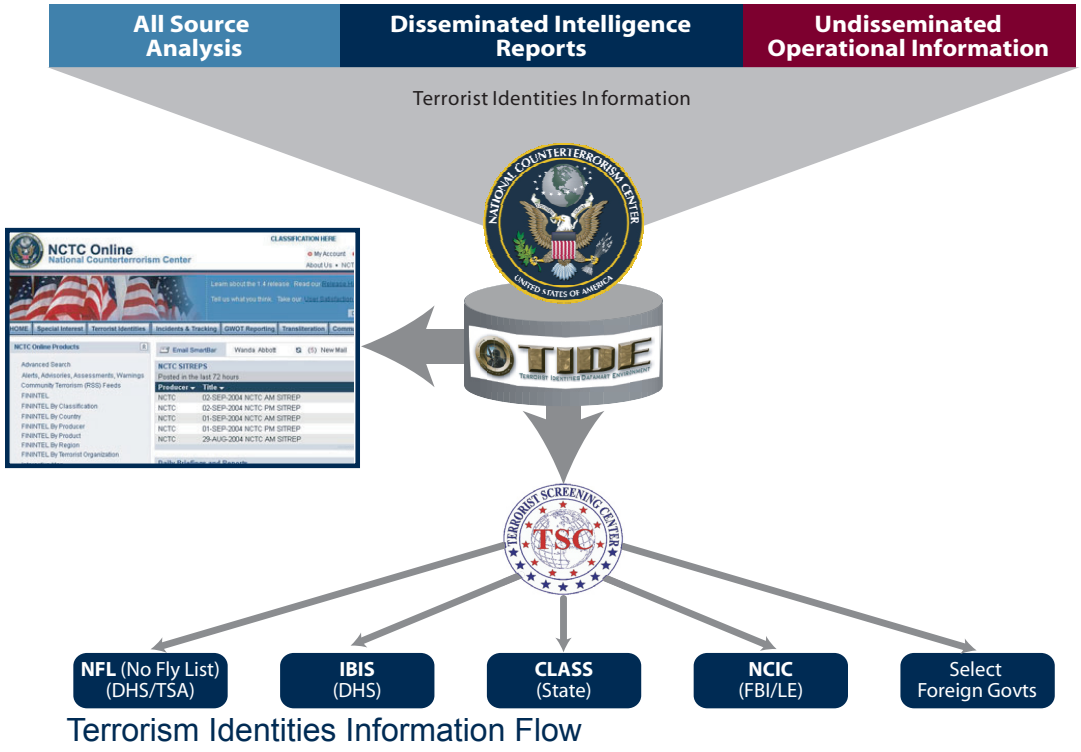
PRIOR TO 9/11

There were numerous classified databases and an approximately a dozen unclassified watchlists containing information about known and suspected international terrorists. These databases and watchlists were neither interoperable nor broadly accessible.

TODAY

The Terrorist Identities Datamart Environment (TIDE) serves as the central knowledge base for all-source information on international terrorist identities for use by the US counterterrorism community. TIDE distributes a "sensitive but unclassified" extract to the Terrorist Screening Center (TSC). The TSC, in turn, validates this information and provides it to Federal departments and agencies and select foreign governments that use this information to screen for terrorists.

- TIDE contains over 400,000 names/aliases, representing over 300,000 unique individuals.
- To further increase information sharing and decrease the potential for "false positives," additional identifiers are passed to the TSC to aide in screening opportunities.
- TIDE is made available to the majority of the terrorism analytic community via NCTC Online.



Terrorism Identities Information Flow

MANY DIFFICULT ISSUES REMAIN

The advancements noted in this report notwithstanding, NCTC and its community partners continue to address many difficult issues:

Privacy—some information vital to the war on terror is intermixed with information about US persons. Ways to use such data while protecting privacy and civil liberties must be identified.

Access—decisions regarding access to information are largely controlled by collectors, thereby creating an inherent tension with analytic elements that need to review information.

Sources and Methods—collectors' ability to obtain vital data must be protected as ways are sought to ensure that intelligence is available to those who need it.

Operational Impact— dissemination of operationally sensitive information must be balanced against the potential adverse impact on intelligence/law enforcement operations.

Liaison information—US law and policy often are not the only factors governing the ability to share information. Key allies may dictate the extent to which their information may be shared. Violating such guidance could result in the loss of future access to information.

Source Credibility—the act of dissemination lends credibility to information and can force operators to respond to very low credibility information. When information meets dissemination criteria, it should include a clear, standardized credibility assessment.

Information Technology—broad information sharing is a double-edged sword. Consumers of information find themselves quickly overwhelmed by the vast quantity of information. Obtaining tools to search, analyze, and process results is critical.

Access to State, Local, and Tribal Governments and the Private Sector—methods for ensuring that homeland security and terrorism information is shared among non-Federal government entities and the Federal government remain inadequate. The Program Manager for the Information Sharing Environment is working to facilitate two-way information flow.

Data Acquisition—acquiring data that contains terrorism information is often a legally and bureaucratically cumbersome process. Often Secretary-level government officials must approve the data transfer; generally only after many layers of review.

Resolving these issues will require managing an extremely complicated balance between technical, legal, policy, and security issues.

NATIONAL COUNTERTERRORISM CENTER