Università
Ca'Foscari
Venezia
Facoltà
di Lingue
e Letterature
Straniere

Corso di Laurea Magistrale in Relazioni Internazionali Comparate (International Relations)

Prova Finale di Laurea

The Turn of the Role of Intelligence after 9/11

Relatore
Ch. Prof. Matteo Legrenzi

Correlatore
Ch. Prof. Duccio Basosi

Laureanda
Giulia Pigato
Matricola 821863

Anno Accademico
2012 / 2013

Un ringraziamento è doveroso a quanti, in ambito personale, accademico, e lavorativo hanno sostenuto il percorso che ho deciso di intraprendere, contribuendo con pazienza, costante fiducia e prezioso incoraggiamento alla sua realizzazione.

"A President has to know what is going on all round the world in order to be ready to act when action is needed… The war taught US this lesson – that we had to collect intelligence in a manner that would make information available where it was needed and when it was wanted, in an intelligent and understandable form"

- Harry S. Truman

INDEX

ACRONYMS

Symbol	Definition
AIT	Advanced Imaging Technology
CBP	Customs and Border Protection
CD	Counterintelligence Division (FBI)
CIA	Central Intelligence Agency
CID	Criminal Investigative Division (FBI)
CRCL	Office for Civil Rights and Civil Liberties
CTC	Counterterrorism Center (CIA)
CVE	Countering Violent Extremism
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNDO	Domestic Nuclear Detection Office
DNI	Director of National Intelligence
DoD	Department of Defense
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
HUMINT	Human Intelligence
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICE	Immigration and Customs Enforcement
IMINT	Imagery Intelligence
INR	State Department Bureau of Intelligence and Research
INS	Immigration and Naturalization Service

NCCIC	National Cyber security and Communications Integration Center
NCPC	National Counter Proliferation Center
NCPS	National Counter Proliferation Center
NCTC	National Counterterrorism Center
NGA	National Geospatial Intelligence Agency
NIC	National Intelligence Council
NIEs	national intelligence estimates
NIP	National Intelligence Program
NIPP	National Infrastructure Protection Plan
NSA	National Security Agency
NSC	National Security Council
NSI	Nationwide Suspicious Activity Reporting Initiative
NTAS	National Terrorism Advisory System
OHA	Office of Health Affairs
PCSC	Preventing and Combating Serious Crime
RFU	Radical Fundamentalist Unit (FBI)
SIGINT	Signals Intelligence
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSP	Terrorist Surveillance Program
TTIC	Terrorist Threat Integration Center
UBLU	Usama Bin Laden Unit
USCG	U.S. Coast Guard
VSP	Visa Security Program
VWP	Visa Waiver Program
WHTI	Western Hemisphere Travel Initiative
WMD	Weapons of Mass Destruction

ABSTRACT

Che cos'è l'intelligence? La maggior parte dei libri che tratta quest'argomento inizia con questa domanda. Sebbene le definizioni fornite siano molteplici, per la maggior parte delle persone, l'intelligence è sinonimo di informazione segreta. Quest'affermazione però non è del tutto vera. L'intelligence è l'informazione che risponde alle esigenze dei politici ed è raccolta, trattata e ridotta al fine di soddisfare tali esigenze. Si può dire che l'intelligence è un sottoinsieme della più ampia categoria delle informazioni.

La decisione di affrontare il tema della svolta del ruolo dell'intelligence dopo l'11 settembre, è sorta dall'importanza e dall'attualità di tale problema. La fase in cui sono entrati gli USA e, assieme a loro il resto del mondo, non è ancora finita, anzi si trova in un processo di continua evoluzione.

Durante la Guerra Fredda, i Servizi Segreti dei diversi Paesi e gli strumenti che avevano a disposizione erano tarati in funzione di un nemico certo le cui mosse erano costantemente monitorate. Oggi invece il nemico è elusivo, imprevedibile ed invisibile. I suoi fattori di potenza non sono più armate possenti, aerei e flotte da battaglia ma bensì la psicologia, le intenzioni, le strategie e le tattiche. Le risposte convenzionali sono ormai inefficaci contro entità sfuggenti e senza territorio quali sono i terroristi. Le trasformazioni che hanno avuto luogo nel sistema internazionale negli ultimi anni sono così minuscole da rendere desuete molte regole e procedimenti sui quali è basata tradizionalmente la politica e in particolar modo quella estera. Gli USA si trovano in quella che è definita politica "post-internazionale", una politica che non si svolge più soltanto tra Stati ma tra i loro sottoinsiemi. Tale politica è caratterizzata principalmente dall'incertezza, che sostituisce la prevedibilità del periodo bipolare.

Oggi, il sistema internazionale è sensibile ad eventi che possono essere considerati apparentemente minori ma che possono dar forma a gravi conseguenze. In parole povere anche un singolo individuo o un piccolo gruppo

possono causare danni enormi e l'attentato dell'11 settembre ne è la prova. Anche se gli obiettivi statali dell'intelligence come Iran, Corea del Nord, Cina e Russia rimangono, il movimento di terroristi e di altre questioni transnazionali è la principale fonte di preoccupazione.

Molti dei principali attacchi terroristici internazionali, compresi quelli dell'11 settembre sono stati concepiti, progettati e lanciati da molti paesi diversi, rendendo le azioni di ogni singolo governo o servizio di intelligence inefficaci alla loro individuazione, dissuasione e prevenzione. Crescente attenzione è stata data ai cosiddetti "temi di ricerca strategica", come l'estremismo islamico e la radicalizzazione, il terrorismo, le minacce strategiche emergenti dalla droga transnazionale, la criminalità, i gruppi finanziari illeciti, e la proliferazione delle varie tecnologie di armi.

Dopo gli attentati dell'11 settembre, i consumatori di intelligence sono aumentati in maniera esponenziale. Questo significa che le questioni transnazionali hanno portato a una più ampia varietà di consumatori, che va ben oltre le agenzie dell'organizzazione della sicurezza nazionale tradizionale e il governo federale. A causa della natura immensa ed estremamente diversificata delle minacce transnazionali, l'intelligence si è trovata ad affrontare una grande quantità di informazioni rispetto a quelle più limitate che erano disponibili da società chiuse come era l'Unione Sovietica. L'unico modo per dominare tale mutamento e vincere la turbolenza causata da questi eventi, è quello di cercare di apprendere e adattarsi alle nuove situazioni. Questa dominazione implica la capacità di analisi, previsione e pianificazione da parte dell'intelligence, ossia la capacità di analisi strategica.

In risposta agli attacchi dell'11 settembre, per merito del Presidente Bush è stato creato il Programma di Sorveglianza del Terrorismo, il quale ha autorizzato che l'Agenzia di Sicurezza Nazionale potesse intercettare telefonate ed e-mail dentro e fuori gli Stati Uniti. Il cosiddetto "sense-making" è definito come il processo attraverso il quale le organizzazioni cercano di comprendere l'ambiente con cui devono lottare. Lo sforzo di capire o dare un significato a ciò che sta accadendo nell'ambiente esterno è continuo. Il sistema di "sense-making" richiede forme di

analisi e di interazioni con consumatori che non sono ancora ben conosciuti, sviluppati o ampiamente utilizzati.

Durante tutto il periodo della Guerra Fredda, l'intelligence dipese in modo particolare dai dati raccolti sia da spie umane sia da attività tecniche di raccolta. L'attuale gruppo di minacce transnazionali richiede l'utilizzo e l'integrazione di tutte le fonti a disposizione degli analisti: giornali locali, discorsi, pubblicazioni accademiche e riviste, le quali forniscono informazioni sul modo di agire e di pensare di una società. Tale conoscenza è molto importante e può fare la differenza quando si tratta di valutare e lavorare su una minaccia.

La strategia di deterrenza che era usata durante la Guerra Fredda è stata ora sostituita da una nuova strategia preventiva, che richiede enorme precisione da parte dell'intelligence. Il diritto di "prelazione", definito come l'uso della forza preventiva a fronte di un attacco imminente, è stato riconosciuto come legittimo e appropriato ai sensi del diritto internazionale.

Negli attentati dell'11 settembre 2001, il governo americano ha interpretato la sua politica dichiarata di prelazione come un avvertimento che è servito sia agli amici sia ai nemici; un avvertimento ignorato da Saddam Hussein e che ha portato alla sua distruzione.

La domanda più frequente dopo l'11 settembre è stata "Perché la CIA e l'FBI non hanno cooperato meglio prima dell'11 settembre?" La verità è che gli americani temevano che la concentrazione del potere dell'intelligence e della polizia avrebbe violato la libertà e la privacy dei cittadini, per questo non sostenevano una loro collaborazione.

Nonostante le indagini del Congresso del 1970 avessero deciso che le due agenzie non dovevano lavorare vicine ci fu una cooperazione abbastanza buona durante la fase finale della Guerra Fredda. Il prezzo della mancata cooperazione tra la CIA e l'FBI dopo la fine della Guerra Fredda, è diventato molto alto a seguito dell'11 settembre, e ha portato la nazione a ripensare all'insieme delle distinzioni organizzative e dei vincoli procedurali che erano stati sviluppati durante la Guerra Fredda.

Verso la metà del 1970 la minaccia comunista sul fronte interno era quasi scomparsa. Da molti punti di vista, l'antiterrorismo risponde alle due missioni classiche di controspionaggio e di applicazione del diritto penale. Si può dire che la lotta al terrorismo ha molto in comune con le operazioni contro la criminalità organizzata e i trafficanti di droga. La sola differenza è che i criminali vogliono vivere per la loro causa e non morire per essa; vogliono vivere al fine di rubare un altro giorno. I terroristi, al contrario, sono pronti a morire per la loro causa. Questo è ciò che spinge l'intelligence a tornare sul tema della prevenzione o prelazione. Un'altra differenza tra la lotta contro il terrorismo e contro la criminalità è che i potenziali terroristi devono essere fermati prima che colpiscano, per questa ragione, la decisione di organizzare le operazioni deve essere presa in precedenza. Poiché i terroristi non devono essere autorizzati a colpire è necessario che siano trovati e fermati prima di agire. La lotta contro di loro è davvero rischiosa. Gli eventi dell'11 settembre 2001, hanno dimostrato chiaramente che il terrorismo internazionale costituisce una grave minaccia per la sicurezza nazionale e hanno portato a una rivalutazione della cooperazione e dello scambio di informazioni tra tutte le principali forze dell'ordine e agenzie di intelligence. Dopo gli attentati, il Congresso ha cominciato a rimuovere le barriere tra le varie agenzie e, soprattutto, ha cercato di garantire che le informazioni disponibili da fonti delle forze dell'ordine, fossero rese accessibili alle agenzie dell'intelligence.

I confini che durante la Guerra Fredda hanno permesso di sostenere le nazioni democratiche, proteggendo la privacy dei cittadini, in un'epoca di terrore, invece, hanno portato quelle nazioni a fallire dal momento che i terroristi non hanno rispetto di nessun confine. Come detto in precedenza, gli obiettivi dei terroristi non sono più gli eserciti ma cittadini privati.

A differenza della Guerra Fredda ora ci sono non solo più obiettivi, ma anche più informazioni e più consumatori.

La legge del 2004 ha iniziato un rimodellamento dell'intelligence. Ha proposto la creazione di centri nazionali di intelligence sotto l'autorità del Direttore dell'Intelligence Nazionale, organizzati per missioni o temi.

In un modo insolito, la Commissione dell'11 settembre ha portato la riforma dell'intelligence americana verso un nuovo territorio. La sua principale raccomandazione è stata il rimodellamento dell'organizzazione dell'intelligence degli Stati Uniti. La Commissione sull'11 settembre, stranamente, invece di scomparire subito dopo la sua emanazione, è rimasta presente, incitando l'amministrazione Bush e il Congresso stesso affinché qualcosa cambiasse. Le famiglie delle vittime dell'11 settembre, le quali non volevano essere ignorate, hanno aggiunto influenza politica alla Commissione ed è grazie a loro se la Commissione è stata istituita.

Tra l'emanazione della Commissione sull'11 settembre e la promulgazione della legge di riforma dell'Intelligence del 2004, non vi era una continuità nel dibattito pubblico in merito alle raccomandazioni. Col senno di poi è facile scoprire le opportunità mancate che avrebbero potuto impedire gli attacchi e giungere ad una conclusione che il mancato prevenirle è stato il risultato di errori sistematici nell'intelligence delle nazioni e negli apparati di sicurezza.

La relazione della Commissione dimostra la difficoltà politica, psicologica e operativa nel prendere misure efficaci per prevenire un tipo di attacco mai avvenuto prima. Prima della relazione della Commissione sull'11 settembre, la sensazione era che l'incapacità di impedire gli attacchi fosse collegata alla mancata integrazione di tutti i pezzi di informazioni posseduti dai servizi di sicurezza su Bin Laden, Al-Qaeda e il terrorismo islamico in generale. Anche se tutti i pezzi fossero stati collegati, ci sarebbe stata solo una piccola possibilità di prevenire gli attacchi.

Descrivendo la difficoltà politica e psicologica di prendere sul serio le minacce che non si sono materializzate in passato, le raccomandazioni della relazione della Commissione sono dirette verso la prevenzione.

La principale proposta della Commissione sull'11 settembre è stata la creazione di una nuova figura: il Direttore dell'Intelligence Nazionale. La posizione del Direttore dell'intelligence Centrale sarebbe stata quindi abolita e non ci sarebbe più stato un solo funzionario sia a capo della CIA sia come presidente di tutta la comunità dell'intelligence. Il Direttore dell'intelligence Nazionale sarebbe diventato l'amministratore delegato della comunità dell'intelligence. Il suo compito principale

sarebbe stato quello di superare la riluttanza delle varie agenzie di intelligence di condividere le informazioni riguardanti le attività terroristiche e di farle cooperare.

In secondo luogo, il Direttore dell'intelligence Nazionale avrebbe dovuto gestire il programma di intelligence nazionale e supervisionare le agenzie che compongono la comunità dell'intelligence. Avrebbe dovuto presentare un budget unificato per l'intelligence nazionale che riflettesse le priorità scelte dal Consiglio di Sicurezza Nazionale.

Dopo gli attentati dell'11 settembre 2001, gli Stati Uniti hanno compiuto importanti progressi per proteggere la nazione dal terrorismo. Il governo federale ha cercato di sviluppare un quadro di sicurezza per proteggere il Paese da attacchi su larga scala. Tale quadro ha portato a un notevole successo sia nella prevenzione per questo tipo di attacco sia nella limitazione della capacità operativa del gruppo di Al-Qaeda. Tuttavia, le minacce terroristiche persistono e continuano ad evolversi, e il lavoro da svolgere è ancora tanto. Oltre alle minacce che provengono dall'esterno, la nazione deve fare i conti con quelle interne.

Negli ultimi anni, il Dipartimento della Sicurezza Nazionale ha lavorato per rafforzare e far evolvere la sicurezza degli USA. All'interno del governo federale, molti dipartimenti e agenzie contribuiscono alla missione di sicurezza interna.

Un'analisi alla storia degli attacchi a sorpresa può essere utile per trovare approcci organizzativi alternativi, perché come è noto, è stato il timore degli attentati che ha mosso l'idea di una riorganizzazione. Tutti gli attacchi a sorpresa seguono un modello, e anche gli attacchi dell'11 settembre ne hanno seguito uno. Una volta definito il modello, la questione è se la riorganizzazione del sistema dell'intelligence è una risposta sensata alla minaccia di attacchi simili.

Prima dell'11 settembre il più grande attacco a sorpresa fu quello giapponese a Pearl Harbor nel 1941. Roberta Wohlstetter, nel suo libro, cerca di spiegare le cause dei fallimenti dell'intelligence USA che hanno portato l'attacco a sorpresa del 1941. All'inizio del 1968, durante il periodo di vacanza del Tet, gli Stati Uniti sono rimasti scioccati da un'offensiva delle forze Viet Cong e dei nordvietnamiti contro le città del Sud del Vietnam. Un terzo esempio di un attacco a sorpresa successo

prima dell'11 settembre fu fatto da Egitto e Siria contro Israele nel 1973, durante la festa ebraica dello Yom Kippur.

Anche se i quattro esempi hanno caratteristiche in comune, sono troppo poche perché dimostrino la loro influenza in attacchi a sorpresa di successo. Analizzando i fatti, ciò che emerge è che gli attacchi a sorpresa non possono essere evitati in modo efficace, e poiché alcuni attacchi possono essere evitati mentre altri no, per quelli che avvengono la miglior cosa da fare è quella di attenuarne le conseguenze.

Dopo aver esaminato gli attacchi a sorpresa di successo e le difficoltà che spiegano il successo di tali attacchi è il momento di prendere in considerazione se alcune di queste difficoltà possono essere superate da una riorganizzazione del sistema di intelligence, dalla messa a fuoco delle raccomandazioni della Commissione sull' 11 settembre e dalla loro attuazione legislativa. Ciò che emerge è che l'incapacità di anticipare gli attentati dell'11 settembre non sembra imputabile al sistema di organizzazione di intelligence degli Stati Uniti . Gli sforzi di completa riorganizzazione amministrativa, come altri programmi governativi, sono i simboli della possibilità di azioni efficaci, ma la soluzione di una riorganizzazione può essere una risposta discutibile ad un problema che non è un vero problema di organizzazione.

La principale accusa della Commissione sull'11 settembre per quanto riguarda la mancata anticipazione degli attentati riguardava l'insufficiente condivisione di informazioni tra le diverse agenzie. Si pensava che una struttura più centralizzata di intelligence sarebbe stata indispensabile per la sua "cura".

La cosa migliore da fare, in ogni caso era quella di acquisire più informazioni possibili in modo da formulare una previsione corretta. Poiché gli attacchi a sorpresa sono eventi a bassa probabilità, tendono a verificarsi a lunghi intervalli. Ogni mese che passa senza un attacco agli Stati Uniti, la vigilanza dei servizi dell'intelligence diventa sempre più debole. Tale intervallo in continua crescita porta a sperare che il pericolo maggiore sia passato.

Una prevenzione più efficace degli attacchi a sorpresa piuttosto che una riorganizzazione del sistema di intelligence potrebbe essere una politica di guerra preventiva progettata per prevenire attacchi a sorpresa.

Le raccomandazioni della Commissione che hanno creato il DNI e il Centro Nazionale sull'Antiterrorismo sono state oggetto di una forte ondata di critiche.
Alcuni critici hanno sostenuto che la Commissione fosse stata riduzionista nella sua attenzione sulla riforma dell'intelligence. Il fatto che molti fallimenti governativi, estranei alla comunità dell'intelligence si siano verificati prima dell'11 settembre non significa che la comunità dell'intelligence stessa non abbia fallito. La debolezza dei governi in altri settori significa che vi è la necessità di migliorare le attività di controterrorismo.

Una riforma dell'intelligence è fondamentale per migliorare le prestazioni di ogni attività dell'organo esecutivo contro il terrorismo. E' impensabile aspettarsi che la comunità dell'intelligence possa fermare tutti gli attacchi terroristici. Tuttavia, il fatto che la comunità dell'intelligence non potrà mai attuare in modo perfetto non giustifica i problemi presenti al suo interno.

Altri critici hanno sostenuto che solo se il personale a servizio dell'intelligence fosse stato migliore, i problemi della comunità dell'intelligence potevano essere risolti. La presenza di personale competente è il presupposto più importante per il successo di un'organizzazione. Tuttavia, nemmeno il migliore personale può fare funzionare una struttura organizzativa in modo perfetto.

Diversi critici erano preoccupati poiché la Commissione non aveva tenuto conto di importanti cambiamenti nella comunità dell'intelligence dall'11 settembre. L'ultima ondata di critiche ha rilevato che una riforma strutturale non avrebbe comunque risolto tutti i problemi della comunità dell'intelligence.

Ciò che è veramente importante è che la comunità dell'intelligence, per una serie di motivi, non è riuscita a mettere insieme una serie di informazioni che avrebbero potuto migliorare notevolmente le possibilità di prevenzione del piano di Osama Bin Laden per attaccare gli Stati Uniti l'11 settembre 2001. Nessuno saprà mai cosa sarebbe successo se più collegamenti fossero stati disegnati tra le

diverse informazioni. Non si saprà mai in che misura la Comunità sarebbe stata in grado di sfruttare pienamente tutte le opportunità che ha mancato. La Comunità dell'intelligence continuerà a migliorare l'integrazione dell'intelligence per usare in maniera più efficiente ed efficace i punti di forza e le capacità che sono sparse nelle sue diciassette organizzazioni.

La comunità dell'intelligence prosegue con i suoi investimenti per combattere il terrorismo e sostenere la Strategia Nazionale dell'Amministrazione dell'antiterrorismo. Al fine di proteggere in modo migliore la sicurezza nazionale, la comunità dell'intelligence rafforzerà le sue capacità di raccolta e di analisi e promuoverà la collaborazione tra le varie agenzie e la condivisione delle informazioni.

In futuro, la sicurezza nazionale non sarà semplicemente la sicurezza dello stato-nazione, ma sarà invece la sicurezza di un sistema pluralizzato di governo, attraverso il quale i cittadini saranno in grado di diffondere la loro lealtà e ricorrere alla sicurezza.

INTRODUCTION

Defining in a proper way the term intelligence is the first step to take in order to contextualize the subject in a socio-political context. More and more often, it happens that the term intelligence is used in an improper way. Such poor attention on the meaning of the term, contributed to produce a dangerous confusion among the public opinion that often referred to intelligence as to the so-called Secret Services or, even worse, to a world made up of spies and deceits. As Robert David Steele[1] asserts, a distinction has to be done among data, which are made up of a text, the signal or raw image; information, which is made up of generic data put together; and intelligence, which is made up of information that has been adapted to support a specific decision of a specific person about a specific issue in a specific moment. In other words, intelligence is the added value given to information so that the one who has to decide could take the better choice among the possible alternatives. The discussion that follows is drawn from Mark Lowenthal's book, *Intelligence: From Secrets to Policy.* In his work, Lowenthal defines intelligence in three ways.

Intelligence as a process: the mean by which certain types of information are required and requested, collected, analyzed, and disseminated, and the way in which certain types of covert action are conceived and then conducted.

Intelligence as an organization: entities that carry out different functions for Intelligence.

Intelligence as a product: a knowledge product resulting from analyses and intelligence operations themselves.

To most, intelligence is information that is kept secret, but this assertion misses a fundamental point. "Information is anything that can be known, regardless of how it is discovered".[2] Intelligence is information that meets the stated or understood needs of policy makers, and has been collected, processed, and

[1] See Steele R. D., *Intelligence – Spie e Segreti in un Mondo Aperto,* Rubbettino, Soveria Mannelli, 2002, p. 284

[2] Mark M. Lowenthal, *Intelligence From Secrets To Policy*, CQ Press College, 2011, p. 1

narrowed in order to meet those needs. It can be said that intelligence is a subset of the wider category of information. “Intelligence and the entire process by which it is identified, obtained, and analyzed responds to the needs of policy makers.”[3] It can be said that all intelligence is information but not that all information is intelligence. The term intelligence refers to issues related to defense and foreign policy and certain aspects of homeland security. The main areas of concern are actions, policies, and capabilities of other nations and non-state groups (e.g. terrorist organizations). Moreover, policy makers and intelligence officers must keep track of powers that are belligerent, neutrals, friends, or even allies that are rivals in some contexts. Intelligence exists because governments want to hide some information from other governments that try to discover hidden information by means that they wish to keep secret.

As Lowenthal points out, even though many aspects of intelligence deserve to be kept secret, this does not prevent describing basic roles, processes, functions, and issues.

Most people tend to think of intelligence in terms of military information. This is just a component of intelligence, but political, economic, social, environmental, health, and cultural intelligence also provides important inputs to analysts. Policy makers and intelligence officials must also consider intelligence activities based on threats to internal security like subversion, espionage, and terrorism. Significantly, “Intelligence is not about truth”.[4] If something were known to be true, states would not need the help of intelligence agencies. The best way to think of intelligence is as an approximate reality. “Intelligence agencies face issues or questions and do their best to reach a firm understanding of what is going on.”[5] They can rarely be sure that even their best analysis is true. Their aims are intelligence products that are reliable, neutral, and free from politicization.

[3] Ibid., p.1
[4] Ibid., p. 6
[5] Ibid., p. 7

◦ The Intelligence Cycle

How is intelligence produced by a series of raw data or information that the most of times have no apparently connection? The most important thing is to outline the development phases of the so-called "informative process", in other words that path made up of a series of conceptual, organizational and executive activities which outcome is a prompt, full of intuit and pertinent, able to support a decision.

Source: https://www.cia.gov/library/publications/additional-publications/the-work-of-a-nation/work-of-the-cia.html

The intelligence cycle is the process of developing raw data into polished intelligence for the request of policymakers. The intelligence cycle is made up of five steps, which are described below. Figure 1 illustrates the circular nature of this process, even though movements between the different steps are fluent. "Intelligence uncovered at one step may require going back to an earlier step before moving forward."[6] This process ensures the job is done correctly as the work is done through a system of checks and balances.

[6] Available at: http://www.fbi.gov/about-us/intelligence/intelligence-cycle

Planning and Direction: it is the phase where objectives and needs are defined. Planning and direction are responsible to identify requirements in order to define those policy issues or areas to which intelligence is expected to make a contribution, as well as taking decisions about the priority between the issues. It may also mean specifying the collection of certain types of intelligence. Intelligence capabilities are always limited, so priorities must be set, with some requirements getting more attention, some getting less, and some perhaps getting little or none at all. Planning and direction are not only the beginning of the cycle but also the end because current and finished intelligence, which supports decision-making, generates new requirements.

Collection: once requirements and priorities have been established, the necessary intelligence must be collected. All information is collected openly or secretly. Some requirements will be better found with specific types of collection; some, instead, may require the use of several types of collection. Taking these decisions among always-constrained collection capabilities means to know how much can or should be collected to meet each requirement.

Processing and Exploitation: collection produces information, not intelligence. Such information must then be processed and exploited before being usable for analysts. Conversion of a large amount of data into a form suitable for the production of finished intelligence is done through several methods including translations, decryption, and data reduction.

Analysis and Production: identifying requirements, conducting collection, processing and exploitation have no meaning until the intelligence is given to expert analysts who can turn it into reports that respond to the needs of the policy makers. The major issues are the quality of the analysis and production, the types of products chosen and the continuous tension between current intelligence products and longer-range products. Analysis and production includes the integration, evaluation, and analysis of all available data, and the preparation of a variety of intelligence products. In this way, the information is logically integrated, put in contest and used for the production of both “raw” and finished intelligence. Usually, “raw” intelligence is referred to individual pieces of information disseminated

individually while finished intelligence puts information in context and draws conclusions about its implications.

Dissemination: the last step is the distribution of raw or finished intelligence to the policymakers whose needs gave start to the intelligence requirements. There should be a dialogue between policy makers and producers after the intelligence has been received, in order to give the intelligence community some sense of how their work has been done and to discuss any adjustments that need to be made. Moreover, finished intelligence over an issue may lead to new requirements by policymakers, and start the whole process again.

◦ The 1947 Act

The Intelligence Community is a federation of executive agencies and organizations that work separately or together to conduct intelligence activities in order to organize foreign relations and protect the national security of the United States. The Act ordered a major reorganization of the foreign policy and military establishment of the U.S. Government. The basic structure of the International Community has been strikingly stable since its establishment in the National Security Act of 1947. The Act is considered to be a historic piece of legislation. It can be seen as critical juncture in the history of American democracy. With the creation of the CIA and prioritization of intelligence and national security, the act signaled a new era in government secrecy and covert operations.

Signed in July 26, 1947 by US President Harry S. Truman, the National Security Act realigned and reorganized the United States armed forces, foreign policy, and Intelligence Community apparatus in the aftermath of World War II. In a particular way, the Act merged the United States Department of War and the United States Department of the Navy into the United States Department of Defense headed by the Secretary of Defense. It also established the National Security Council, a central place of coordination for national security policy in the Executive Branch, and the Central Intelligence Agency, the first peacetime intelligence agency of the United States.

◦ The National Security Council

The National Security Council (NSC) was given the task of coordinating and advising the president on the integration of domestic, foreign, and military policies relating to national security in order to enable the military services and other agencies and departments of the Government to cooperate more effectively on issues regarding national security. The NSC is made up of senior members of the U.S. government, the armed forces, and the intelligence community. This includes, among others, the President, the Vice President, the Secretary of State, the Secretary of defense, the Director of Mutual Security, the Chairman of the National Security Resources Board and the Secretaries and Under Secretaries of the executive and military departments. Given its role as an advisory body to the president, the NSC is a flexible organization.

◦ The Central Intelligence Agency

The Central Intelligence Agency (CIA) grew out of the World War II era. The 1947 Act created the director of central intelligence (DCI) who is in charge of protecting intelligence sources and methods. His role is to coordinate the intelligence activities of the nation and correlate, evaluate, and disseminate intelligence that affects national security. The CIA provides accurate, comprehensive, and timely foreign intelligence on national security topics to the president and to the National Security Council. Moreover, it conducts counterintelligence activities, special activities, and other functions related to foreign intelligence and national security, following the directions of the president.

◦ The Department of Defense

The Department of Defense (DoD) unified the United States Army, Navy, and Air Force under a single cabinet-level secretary, the Secretary of Defense. This integration into one department was considered revolutionary at that time. The secretary of defense has been at the head of the unified army, navy, and air force to the present day. The 1947 Act provided that the Secretary of Defense would report directly to the president. The tasks of the Secretary were to develop general policies for the military and to coordinate defense matters among the separate services.

◦ United States Military Services

The intelligence organizations of the four military services (Air Force, Army, Navy, and Marines) concentrate now largely on concerns related to their specific missions. Their analytical products, together with those of Defense Intelligence Agency, supplement the work of CIA analysts and provide greater depth on key technical issues. The 1947 Act established the United States Air Force as an independent armed service within the Department of Defense. Until that time, the air force was an entity of the army.

The basic U.S. Intelligence structure was kept as it was established until September 11, 2001. The National Commission on Terrorist Attacks Upon the

United States, also known as the 9/11 Commission, made recommendations to restructure the intelligence community. The major change made by the National Intelligence Security Reform Act of 2004 was the creation of the Director of National Intelligence (DNI). The DNI replaced the director of central intelligence (DCI) as the senior intelligence official, head of the intelligence community, and principal intelligence adviser to the National Security Council (NSC) and the President.

Once, intelligence was divided into foreign and domestic intelligence. Now, the term "national intelligence" has emerged to replace the old distinction between foreign and domestic intelligence. The new term includes three subsets: foreign, domestic and homeland security. Such change gave the DNI more responsibilities than the DCI for aspects of domestic intelligence. The Act was done in order to improve a better share of intelligence. The DNI has free access to all intelligence, and is responsible for ensuring that it is disseminated as needed across the intelligence community. He is not connected to any intelligence agency. The head of the Central Intelligence Agency (DCI) is now only the director of the CIA. In addition to his staff, the DNI controls the National Counterterrorism Center (NCTC), a new National Counter Proliferation Center (NCPC), the National Intelligence Council (NIC), and the National Counterintelligence Executive.

◦ The Onset of an Age of Terror

When the first wave of terrorist attacks struck, National-Intelligence services had not yet digested the implications of the end of the Cold War. Such events brought to a reshape of intelligence. The onset of an age of terror focused the role of intelligence services in the detection and prevention of possible terrorists attacks. During that time, a series of investigations focused the attention on the performance of such intelligence services.[7] In the United Sates the reshaping began with the Terrorism Prevention and Intelligence Reform Act of 2004, anyway

[7] The two most detailed investigations in the United States are the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington DC 2004); and the *Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington DC 2005).

the law was just the beginning of the reshaping. With the end of the Cold War and the onset of the Muslim extremist terrorism, the role of intelligence changed seriously. The major differences with respect to the Cold War era are summarized in the following table.

Intelligence From the Cold War to an Age of Terror

	Old: Cold War	New: Age of Terror
Target	States, primarily the Soviet Union	Transnational actors, also some states
"Boundedness"	Relatively bounded: Soviet Union ponderous	Much less bounded: terrorists patient but new groups and attack modes
"Story" about Target	Story: states are geographic, hierarchical, bureaucratic	Not much story: non-states come in many sizes and shapes
Information	Too little: dominated by secret sources	Too much: broader range of sources, although secrets still matter
Interaction with Target	Relatively little: Soviet Union would do what it would do	Intense: terrorists as the ultimate asymmetric threat

Source: Gregory F. Treverton, Intelligence for an Age of Terror, Cambridge University Press, 2009, p. 2

Transnational targets, like terrorists, differ from traditional state targets in many different ways. The changes brought from such events are connected by some common themes.

The first theme is risk. Intelligence has always been as coverage against risk, but now that the threat has changed, so has the nature of the risk. There is always more pressure on intelligence which has to be now not only good enough to

structure deterrent threats but has also to reach in depth small groups, in order to provide an understanding that can bring to preventive action.

The second theme is the corresponding expansion in the intelligence consumers. In the past, intelligence used to be planned mainly for a relatively small piece of political and military states leaders but now it could be useful to a major number of consumers. Intelligence has moved from the "need to know" to the "need to share".[8]

The third theme is the enhanced number of needs for intelligence through a big number of time horizons from instant warning to longer-term comprehension.

The fourth and last theme is both law and organization of boundaries. During the Cold War, democratic societies traced boundaries between law enforcement and intelligence, between public and private and between home and abroad. Boundaries led nations to fail against a terrorist enemy that respected none of such boundaries.

The intent of this work is to analyze the change that took place after the end of the Cold war through the analysis of the different Acts that were made in order to try to reshape intelligence. Such analysis demonstrates that numerous were the attempts to improve the means of intelligence, sometimes with and other times without success.

[8] Gregory F. Treverton, *Intelligence for an Age of Terror*, Cambridge University Press, 2009, p. 3

CHAPTER 1

THE CHANGED TARGET

1.1 INTRODUCTION

The change of targets for intelligence is unbelievable. The stress is put on terrorists and other non-state or transnational targets in order to highlight the absolute degree of change. In the past, Intelligence dealt with non-states and nation-states that still threaten the work of U.S. Intelligence. Some of these state targets are familiar in the sense that they resemble the Soviet Union, others, instead, present different and completely new challenges.

The aim of this chapter is to define such change in targets with attention on transnational targets like terrorists. Such change goes right to the center of the intelligence business. Before starting with transnational targets a look to the remaining state targets is still important because of its continuous presence. The challenges of transnational targets and the consequent possible acquisition of WMD by terrorists are then discussed. The chapter then ends with the main question after September 11, “Why didn’t the CIA and the FBI cooperate better before September 11?” The truth was that the American people feared that the concentration of intelligence power and police would violate the liberty and privacy of the citizens, so they didn’t want them to cooperate. After the congressional investigations of the 1970s in particular, they had decided that the two agencies should not have to be too close.

The failure of September 11, 2001 is the first sense in which the Cold War heredity of intelligence was and is in contrast with the transnational threat that the United States and its allies now have to face.

1.2 THE RANGE OF STATE TARGETS

States will not only remain targets for Intelligence, but also the key actors in the international system. In other words, they "will remain an important target for intelligence."[9] The range of state targets is a continuum and table 2 illustrates three position of interest: closed, mixed and open. As we can see, even the most open states keep some secrets, reminding us that openness is relative.

Closed	Mixed	Open
Soviet Union then, North Korea now	China, Iran now	U.S. allies; much of the world
Basic data on capabilities secret: focus on puzzles	Puzzles about capabilities remain; mysteries important too	Most capabilities transparent; mysteries critical
Secret sources dominate collection; too little information	Secret sources valuable; open sources as well	Secrets less valuable; too much information is a problem

Source: Gregory F. Treverton, *Intelligence for an Age of Terror*, Cambridge, Cambridge University Press, 2009, p. 16

We know what states look like, even if States are so different from the United States as is the Soviet Union or North Korea. They are hierarchical and bureaucratic states. The reason is that their purposes are widely similar, so their internal institutions result similar too. A lot of intelligence questions about states fell into the distinction between puzzles and mysteries. Puzzles could be solved with certainty only with the access to information that is available in principle. The majority of Cold War intelligence was puzzle-solving, this mean that it was possible to complete a mosaic of understanding which broad shape was given. The U.S. spent billions of dollars on exotic collection systems to solve those puzzles because so much that

[9] Gregory F. Treverton, 2009, p. 15

was open about the U.S. and other democracies was instead a secret for the Soviet Union.

Because of the secrecy of those puzzles, their solving relied heavily on secret intelligence sources: espionage (HUMINT) and what came to be called “technical collection” by “national technical means”, (IMINT or SIGINT).[10] Those secret sources, in a special way HUMINT, were combined to puzzle solving. Spies may or not afford to provide useful information about fast-moving intentions or plans. In most cases, however, the missing puzzle piece of today will still be welcome tomorrow. In contrast with puzzles, mysteries cannot be definitively solved because they are not about things but about people. In this case the answer cannot be known, but it can be known which factors are important to control and how they interact in order to produce the answer. While for puzzle the product is the answer, for mysteries the product is a best prevision, maybe in the form of a probability with key issues as well as how they are relevant on the estimate.

[10] Ibid., p. 17

1.3 TRANSNATIONAL ISSUES

Transnational targets, like terrorist, differ from traditional state targets in many different ways. Such differences are illustrated in the table 3.

From Cold War Targets to Age of Terror Targets

	Old: Cold War	New: Era of Terror
Target	States, primarily the Soviet Union	Transnational actors, also some states
Objects of Scrutiny	Mostly big, rich and central	Many small, even single individuals, and peripheral
"Story" about Target	Story: states are geographic, hierarchical and bureaucratic	Not much story: non-states come in many sizes and shapes
Location of Target	Mostly "over there", abroad	Abroad and at home
Consumers	Limited in number: primarily federal, political military officials	Enormous numbers in principle: including state, local and private
"Boundedness"	Relatively bounded: Soviet Union ponderous	Much less bounded: terrorists patient but new groups and attack modes
Information	Too little: dominated by secret sources	Too much: broader range of sources, although secrets still matter
Interaction with Target	Relatively little: Soviet Union would do what it would do	Intense: terrorists as the ultimate asymmetric threat
Form of Intelligence Product	"Answer" for puzzles; best estimate with excursions for mysteries	Perhaps "sensemaking" for complexities
Primacy of Intelligence	Important, not primary: deterrence not intelligence-rich	Primary: prevention depends on intelligence

Source: Gregory F. Treverton, *Intelligence for an* Age of Terror, Cambridge**,** Cambridge University Press, 2009, p. 22

These targets are not new for intelligence because in the past it has been active against drug traffickers and organized crime. The two new themes that emerge are the importance of transnational threats, in particular way terrorism, even though it is not the only one, and the variety of transnational threats of concern.

In the past, drug traffickers and organized crime were a secondary activity in the intelligence work; now, some transnational threats like terrorism are the main activity. The range of current and prospective transnational targets is wide. Threats can be considered as covering a range if threat is considered widely. At one hand are those threats that come with "threateners" attached, people who have the intention to harm us. At the other hand are developments that can be tough of as threats without "threateners". If they are a threat, the threat results from the cumulative effect of actions taken for other reasons, not from an intent that is purposive and hostile. They might also be called systemic threats.

> *Those who burn the Amazon rain forests or try to migrate here or who spread pandemics here, or even those who traffic in drugs to the United States, do not necessarily wish Americans harm; they simply want to survive or get rich.*[11]

In contrast with the past, where the targets were big, central and rich, now, many objects of scrutiny for intelligence are small, peripheral and poor. In an age of terror, even a single individual or a small group can do massive damage, and the September 11 hijackers is the proof of it.

In a similar way the places to which intelligence has to turn its scrutiny have also changed. Many of them are peripheral and poor, like for example Afghanistan. Now that we know enough about terrorists we can say that they are not generally poor, but what we also know is that poor countries are not only fertile ground for the recruitment of terrorists but they can also be chosen by terrorists as bases and safe havens. After the fall of the Soviet Union, the U.S. discretionary interest, driven by the interest of allies or by simple suffering, was no longer in peripheral places. The

[11] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge, Cambridge University Press, 2001, p. 43

intelligence agencies and the U.S. government need to pay attention to peripheral and poor places that can be part of the terrorism threat.

Even though state targets of intelligence, like Iran, North Korea, China and Russia will remain, the move to terrorists and other transnational issues is very important. While states came with some "story" attached, transnational targets, and in a specific way terrorist groups, do not. These new targets are deprived of a shared story that would facilitate intelligence and policy analysis and communication. While we know that states are geographical, hierarchical and bureaucratic, non-states have not a comparable story because they come in many shapes and sizes.

Transnational targets come not only without a story but also without an address, they are both "here", at home, and "over there", abroad. The fact that transnational targets are both "here" and "over there" incite nations to "reconsider what has been considered domestic intelligence."[12] In addition to face the necessity of collecting more information about citizens and residents, they need to rethink the boundaries that the distinction set up. Terrorist groups and international crime organizations have much in common. One crucial difference is that while terrorist may commit only one crime, and then it will be too late, criminals, instead, want to live so they can steal another day, for this reason they are not candidates for suicide bombs.

The world is now confronted with a host of border-spanning trends that challenged traditional law enforcement practices and intelligence. What makes the traditional intelligence model less effective and distinguishes today's tests, is the transnational and global character of many trends. As Tom Friedman's "flatness" metaphor points out, the compression of time and space and the easy movement of people, knowledge weapons, drugs, toxins and ideas have transformed the way threats emerge and challenged the way intelligence must operate.

Many of the major international terrorist attacks, including those of 9/11,

> *follow the model of having been conceived, planned and launched from many different countries, making the individual actions of any single government or*

[12] Gregory F. Treverton, 2009, p. 28

intelligence service ineffective for the detection, deterrence or prevention of those attacks.[13]

Growing attention has been given to the so-called "strategic research themes" such as Islamic extremism and radicalization, terrorism, strategic threats emerging from transnational drug, crime, and illicit finance groups as well as to proliferation of various weapons technologies.

[13] Roger Z. George, *Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm*, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html

1.4 INTELLIGENCE'S CONSUMERS

During the Cold War consumers, besides sharing with intelligence a story about states, were relatively few in number. At that time most consumers were located at the top of the national-security decision-making establishments. Because they were busy and distracted, it was not always easy for intelligence to face those targets. As the Cold War ended, intelligence looked for new consumers and found them at first in domestic agencies.

After the attacks of September 11, intelligence's consumers increased tremendously, including state and local officials and private manger of infrastructures. Therefore, transnational issues involve a wider variety of consumers, extending to agencies outside the traditional national-security organization and outside the federal government.

> *The lack of a story for transnational targets such as terrorists, or the presence of tentative, competing stories about them often based only on short stories, is also compounded by the different organizational cultures involved"*[14]

The majority of states are clearly delineated, meaning that they have known borders and capitals and do much that is publicly observable. In addition, states act in the contest of customary and formal rules, which makes their actions predictable. In opposition, transnational actors are formless, hidden and fluid, and present intelligence with major challenges in the description of their boundaries and structure. Such actors are far less constrained by formal rules than their state counterparts so that they can engage in a major variety of tactics on a regular basis.

Terrorists are hardly open, but a large amount of open data is important for them. During the Cold War intelligence, the problem was that there was too little good information while now there is too much unreliable information. At that time secrets were considered reliable while now the excess on the web is a mixture of

[14] Gregory F. Treverton, 2009, p. 29

fact, fancy and disinformation. Because of the immense and high profile nature of transnational threats, intelligence must face a big amount of information that is in contrast with the more limited information that was available on closed societies like the Soviet Union. In comparison with a state with a long history, there is much less contextual information available that can be used to evaluate the reliability of new information. Considering these reasons, the problem of separating signals from noise is more emphasized in the transnational environment.

The lack of a story means that the collection of information against terrorists necessarily involves the processing of large quantities of information. After the September 11 attacks, when the names of the hijackers were known, the government could have quickly picked up their tracks through motor-vehicle records, credit cards, addresses and similar. Anyway, that was after the fact; before the fact, names of interest may be unknown or difficult to follow because of pseudonyms or different transliterations of the same Arabic name.

In response to the September 11 attacks, President Bush created

> *the Terrorist Surveillance Program (TSP), which authorized the National Security Agency (NSA) to intercept phone calls and emails traveling into and out of the United States.*[15]

The Program illustrated the challenge of dealing with the presence of a big amount of information and the absence of context for processing it. After September 11, "the U.S. government was worried about new plots and cells, but had few specific leads."[16]

The terrorist target is the ultimate asymmetric threat that shapes its capabilities to the victim's vulnerabilities. The September 11 bombers had done enough tactical reconnaissance to know the weakness of defensive passenger-clearance procedures and that fuel-filled jets in flight were a vulnerable resource. It

[15] John Yoo, *The Terrorist Surveillance Program and the Constitution*, George Mason Law Review, Vol. 14, 2007, p.1 available at: http://www.georgemasonlawreview.org/doc/14-3_Yoo.pdf

[16] Gregory F. Treverton, 2009, p. 32

can be said that terrorists' capabilities are a mystery, in the sense that those capabilities depend on their continuing adaptation to their targets' vulnerabilities.

Transnational actors like terrorists have, in contrast to states such as the Soviet Union, a stronger relationship with the dominant actor in the international system, the United States. Their tactics are often affirmed on U.S. defensive and policies measures, and this makes their behavior less predictable and determinate.

> *The understanding of transnational actors' inclinations will lead to take actions that will induce adaptive behavior on their part. Such process of adaptation can change the predictions of intelligence into "self-negating prophecies".*[17]

This interaction has difficult implications for intelligence, in particular foreign intelligence, which has been imposed in many countries for examining the home front and, worried that getting too close to policy is to run the risk of becoming politicized.

The intelligence's task focuses now on the domestic-foreign distinction. As said before, transnational targets include both puzzles and mysteries, but they also involve what might be called a mystery-plus. The hiding place of Al-Qaeda leaders along the Afghanistan-Pakistan border was considered a puzzle, even though its solution might have been easily altered as the leaders moved among hideouts. A mystery instead, is considered with regards to when, where and how Al-Qaeda might attack the United States. The mystery concept seems not to frame the challenge of understanding Islamic extremist terrorism and other transnational targets.

Terrorism involves a big variety of causes and effects that can interact in many different ways. This is due to its relatively little history and context and to its absence of boundaries. A big number of small actors respond to a constant movement of situational factors. Furthermore, they do not repeat in any established model and for this reason are not inclined for predictive analysis in the same way as mysteries.

> *Despite both the September 11 terrorists in 2001 and the Forth Dix plotters in 2006-7 have connections to Al-Qaeda, the links were very different, and the first did not provide any model for the second.*[18]

[17] Ibid., p. 33

The distinction between traditional and transnational intelligence problems should not be exaggerated because there are state-to-state problems as are battlefield situations and crisis diplomacy where interactions among different players can also produce numerous outcomes.

The combination of regional and functional knowledge is required to understand the transnational issues' complexities. In resolving puzzles or mysteries, a country's political or economic analyst can work relatively isolated from analysts with other specializations, but that is not the case for transnational issues. The challenge of dealing with complexities is a constant presence. The aim is to spread a sense of emerging models with attention to reinforce or disrupt, positive or unfavorable patterns. The process runs into two obstacles: the recognized separation of intelligence from policy; and the fact that policy officials, in particular, tend to be hard pressed for time. The perception needs to develop out of a shared analytical work because the problem is not simply communication. The product is what can be called organizational sense making, as noted by Karl Weick, the known organization theorist.[19] The so-called sense making is the process through which organizations understand the environment with which they have to struggle. The effort to understand or make sense of what is going on in the external environment that is relevant to the organization's needs and aims, is continuous, repetitive and largely informal. Thanks to conversations at all levels, organizations can construct continuing interpretations of reality, comparing new events with the past ones, or developing stories to account for them.

The sense-making process creates a unified, consensual and explanatory understanding about the world that brings to consistent, principled action. The system of sense making requires forms of analysis and interactions with consumers that are not yet well known, developed or widely used. The real need is not for good

[18] The Fort Dix plot involved six individuals who planned to attack the base using a variety of military-style assault weapons. It was first noticed by a Clerk at a local video store who saw a video one of the men brought in to be duplicated that contained footage of weapons training and other suspicious activity; the Clerk notified the police.

[19] See Karl Weick, *Sense making in Organizations*, London, Sage Publications, 1995

analysis on a piece of paper but for improved official's understanding that will decide or act, and for analysts' deeper research.

1.5 INTEGRATING TRANSNATIONAL THREAT ASSESSMENTS WITH OPEN SOURCE

As the Cold War national security paradigm threat has changed, the traditional dependence on classified information must change too. During all of the Cold War era, intelligence depended in a special way on data collected both by human spies and by technical collection activities. All data were classified and their use was frequently controlled, and therefore limited, by the groups and agencies collecting the information. Classified information became the analyst's only type of information that could be trusted and valued. The knowledge of the academic community wasn't sufficiently exploited, while no classified materials were often seen as marginal sources.

As discussed before, today's security environment is different from the previous one. The change was first, in the presence of more issues, players, and therefore more complexity; second, in the availability of more destructive technologies; and third, in more access and vulnerability of societies.

The use of open source information is central for the development of high-quality, relevant intelligence appraisals. It was not easy for the intelligence community to recognize the value of open sources and use them. Most states collect and assess secrets relevant to the protection of their national security interests, and this is the reason why they create and sustain intelligence organizations.

> *Since open sources do not provide secrets, the task of collecting and assessing this type of data would appear at first glance not to fit within the understood purpose of an intelligence community.*[20]

Thinking about open sources in this way, means to fail to meet their value. Joseph Nye, during his mandate as chair of the National Intelligence Council, said:

[20] Mark Lowenthal, 2000, p. 5

> *open source intelligence is the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle… open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.*[21]

Secrets identified via human and technical means can be complemented, clarified, framed and supplemented by open source information. While in some situations open source intelligence may help direct a source of classified data or provide information that can be used more in international and public contests, in others, it may eliminate the need for some types of collection activities allowing the redirection of resources toward efforts where the acquisition of classified data is most critical.

The present group of transnational threats requires the use and integration of all available sources from the analysts. Local newspapers, speeches, academic papers and journals, provide the knowledge of a society's way of acting and thinking, a knowledge that could make a difference in how to evaluate and work on a threat. The executive summary of the Aspirin-Brown Commission on the Roles and Capabilities of the U.S. Intelligence suggested that:

> *greater use be made of substantive experts outside the intelligence community. A greater effort also should be made to harness the vast universe of information now available from open sources.*[22]

Without a significant increase in the use of open-source materials in every feature of the intelligence's process of assessment, efforts to prevent and strike-back today's security threats will not succeed.

---

[21] Joseph Nye, *speaking to the members of the Security Affairs Support Association*, Fort Meade, Md., April 24, 1993

[22] Commission on the Roles and Capabilities of the U.S. Intelligence Community, Aspirin-Brown Commission, *Preparing for the 21st century: An Appraisal of U.S. Intelligence, Executive Summary*, Washington D.C., U.S. Government Printing Office, 1996

1.6 THE IMPORTANCE OF INTELLIGENCE

The last major difference between state targets and transnational targets may be the most important. In the 2002 national strategy, President Bush spoke of Iraq but was very clear about the prevention of attacks by preemptive action if needed:

> *We must be prepared to stop rogue states and their terrorist clients before they are able to threaten or use weapons of mass destruction against the United States and our allies and friends ... to forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively.*[23]

In his speech at West Print in June 2002 he had foreshadowed the new strategy: "By confronting evil and lawless regimes, we do not create a problem, we reveal a problem. And we will lead the world in opposing it."[24]

The deterrence strategy of the Cold War was now being replaced by the new preemptive strategy. Such strategy was based on the supposition that for all the differences in aims and ideology, the Soviet Union was like the United States, in other words modern, not self-destructive and rational.

Prevention, whether by disruption, preemption or defending vulnerabilities, needs enormous precision in intelligence. The right of preemption, which is defined as the anticipatory use of force in the face of an imminent attack, has long been accepted as legitimate and appropriate under international law. Although many agree that the warnings of armies that take form along borders no longer subsist and the concept of imminent threat must be adapted to the capabilities and aims of today's adversaries, it is clear that determining the degree of imminence in order to gain the necessary domestic, or even international, support for future preemptive action will be increasingly problematic.

---

[23] *National Security Strategy of the United States of America*, Washington DC, September 2002, pp. 14-15, available at: http://www.state.gov/documents/organization/63562.pdf

[24] George W. Bush, *Graduation Speech at West Point*, 1 June 2002 available at: http://georgewbush-whitehouse.archives.gov/news/releases/2002/06/20020601-3.html

With regard or not to the United States self-proclaimed right to preemptive attack in the future, it is clear that its preemptive action in Iraq has had an effect on the international community. The future possibility of the world's only superpower acting in a preemptive way has proven not only painful to its enemies, but also to many of its allies. In the attacks of 11 September 2001, the U.S. government interpreted its stated policy of preemption as a warning served to both friends and foes, a warning ignored by Saddam Hussein that led to his destruction.

If terrorist threats must be prevented by closing the vulnerabilities they seek to exploit or by disrupting them, then big pressure is placed on intelligence to understand threats soon and well enough. This means moving away from the possible terrorist acts to groups and their tendencies or intentions. However, the goal of prevention and deterrence is nothing, no attack.

1.7 THE BAYESIAN APPROACH

The origin of the term Bayesian comes out from a famous theorem discovered by Thomas Bayes. The term then was used to describe both an inclination and a process to update subjective probabilities given new evidence. It can be said that all intelligence analysis is Bayesian, because even with regard to puzzles, finding the piece that solves the puzzle with certainty is rare. However the uncertainty of transnational targets underlines the need for a Bayesian attitude and for more formal approaches, in order to make that approach concrete. The Bayesian approach, as a way of thinking, is even more important for complexities and mysteries because it underlines the inherent uncertainty and forces hard conversation. Also traditional warning is a Bayesian process. Warnings try to turn a mystery into a puzzle by identifying indicators along the path to war and then controlling them. The warning problem requires intelligence from many sources to be put at the top of one other. Both in terrorism and warning, policy measures may increase the Bayesian updating of probabilities by making actions more visible or unique.

The probabilistic character of customary intelligence judgment gives life to the intelligence interest in probability theory. Intelligence analysis must usually start on the basis of incomplete evidence, for this reason, words and phrases as "may," "very likely," "better than even chance," "possibly," and other qualifiers are usually used for conclusions.

This way of allowing for more than one chance let intelligence be of acting the oracle whose prophecies try to cover all contingencies. “The best that intelligence can do is to make the most of the evidence without making more of the evidence than it deserves.”[25]

Very often, the best recourse is to give attention to the probabilities. The focus on such probabilities has led to some research on possible intelligence applications of Bayes' Theorem.

[25] Central Intelligence Agency, Bayes' Theorem for Intelligence Analysis available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol16no2/html/v16i2a03p_0001.htm

The formulation of Bayes' Theorem is the equation: R=PL, where R is the revised estimate of the probabilities favoring one hypothesis instead of another — the estimate of the probabilities after considering the latest point of evidence; and P is the previous appraisal of the probabilities — the probabilities before consideration of the latest point of evidence. After the starting estimate was available, the participating analysts made no judgments about P. It was a value taken back in machine memory from previous analysis. R, the result of the mathematical elaboration, was what went back into machine memory to become the value of P used in consideration of the next evidence point. The participating analysts gave judgments only about L, the probability ratio. Conventional intelligence analysis is distinguished from the Bayesian method by three principal characteristics.

The first distinguishing characteristic is that the analyst does not take the available evidence as given and his conclusions are drawn about the relative merits of opposing hypotheses. The analyst rather postulates the truth of each hypothesis, addressing himself only to the probability that each item of evidence would appear. The analyst feels no need to reinforce his self-esteem by reaffirmation of opinions previously put on the record.

The second distinguishing feature of Bayesian method is that the analyst makes his judgments about pieces of evidence and not as he would have to do if he had to judge its meaning for final conclusions. The mathematics does the summing up. Some Bayesian psychologists' research findings seem to show that people are generally better at appreciate a single item of evidence than at drawing inferences from the body of evidence considered in the aggregate. If these findings are to be considered valid, then the Bayesian approach require the intelligence analyst to do what he can do best and to leave all the rest to the logic of an impassive mathematics.

The third distinctive feature of Bayesian method that the intelligence analyst has to quantify judgments he does not ordinarily express in numerical terms. This characteristic is the one that perhaps draws most of the critics against the Bayesian approach in intelligence analysis. A point of discussion of the critics is that analysts are bound to disagree in their opinions of the exact figure that should represent the

diagnostic value of a unit of evidence. The Bayesian criticism is that disagreement among analysts is just as much a characteristic of the traditional method, and in the analysis, it is no less serious for being implicit rather than explicit. The critic returns to the discussion by observing that the typical analyst finds it extremely difficult to express his degree of belief to the precision implied by a numerical value. The supporters of Bayes take the position that people have been quantifying judgments based on probability since the beginning of time.

The Bayesian approach was not studied with the idea of replacing other approaches in intelligence analysis with it. The task of intelligence is to represent in the best way it can, the present and possible international affairs' state. The intelligence opinion is outlined in all the lights and shadows of narrative, descriptive and interpretive commentary.

> *The intelligence evaluation is a closely reasoned analysis of such important issue of interest as the top political leadership of a foreign country, evolving popular attitudes in that country, changing force structures in its military establishment, its levels of scientific achievement, and the hard choices it is making to allocate resources to the guns and butter sectors of the economy.*[26]

Nevertheless there are areas of intelligence analysis where Bayes' Theorem may well complete other approaches. An important area is the strategic warning one — the analysis directed to discover any activity by a foreign power evoking a major and imminent threat to US security interests. Cases in point are the models of the Communist invasion of South Korea in 1950 and the events leading to Pearl Harbor in 1941. The analysis of strategic warning focuses primarily on the problem with which Bayes' Theorem deals — the odds favoring one hypothesis (forthcoming attack) over another hypothesis (no forthcoming attack).

One way to evaluate the utility of Bayes' Theorem for intelligence analysis is to repeat intelligence history. This means going back to international crises of the past years. It means bring back together the evidence that was available before the ending results of the crises were known. It means reading the old intelligence and

[26] Ibid.

other studies opinions in way of finding out how the analysts of the past interpreted the evidence. It means assignment of L values that reflect these analyst evaluations of the evidence in an honest way. Another way to test Bayes' Theorem is on current income of evidence. The advantage of this test is that looking at the past knowledge does not interfere. Bayes' Theorem is put in competition with the conventional modes of analysis. Compensating this advantage for honest research, anyway, is disabling disadvantage. Such disadvantage derives from the hypotheses' nature at interest in strategic warning. Commonly, the alternative hypotheses are of two types. One draws up continuation of the status quo. The other draws up sudden change from the status quo. The status quo hypothesis, normally, prove to be the true once in strategic warning analysis. But the main test of strategic warning efficacy is the capability to give notice of the sudden changes that now and then do occur in the status quo.

The intelligence interest in Bayes' Theorem is mainly in how well the Bayesian approach to strategic warning would meet this main test of performance in situations of general surprise. Unfortunately, intelligence research cannot be accelerated by focus on the particular current matters, which will change into occasions of intelligence surprise.

If intelligence could choose in advance the matters on which it was going to be surprised, it would never be surprised, and it would not be interested in the possible contributions of Bayes' Theorem to improved analysis. The hypothesis, then, is that many tests of Bayes' Theorem on current influx of evidence will be needed to obtain the few occasions which show Bayesian performance in situations of general intelligence surprise. A large enough sample of interesting examples is needed to justify confident findings of comparative performance on the average. The results of the testing so far have been interesting enough to make a good example for additional testing of Bayes' Theorem in intelligence analysis.

1.8 THE COLD WAR HEREDITY: INTELLIGENCE OR LAW ENFORCEMENT?

The most frequent question after September 11 was "Why didn't the CIA and the FBI cooperate better before September 11?" The truth was that the American people feared that the concentration of intelligence power and police would violate the liberty and privacy of the citizens, so they didn't want them to cooperate. After the congressional investigations of the 1970s in particular, they had decided that the two agencies should not be too close. By the final stages of the Cold War, when early preoccupation about communists connected to Moscow in their midst resulted to be exaggerated, raggedy cooperation between the two agencies was good enough. Anyway, the failure came on September 11, 2001. That is the first sense in which the Cold War Heredity of intelligence was and is in contrast with the transnational threat that the United States and its allies now have to face. The CIA and the FBI are in the middle of the fundamental boundaries of the Cold war, boundaries between intelligence and law enforcement, domestic and foreign, private and public.

The nation thought that as law enforcement was one thing and intelligence another, so too there had to be a decisive distinction between public and private, and between home and abroad. The boundaries were strengthened by the second of the Cold War heredity: the institutional heredity. The majority of what the United States spends on intelligence went and still goes for collection. Satellites and other sophisticated collection platforms are very expensive in comparison with the inexpensiveness of analysts. Collection became organized in "stovepipes", as the government officials called them, and stovepipes were dominated by source. The responsible for HUMINT [27] was the clandestine service or the directorate of

[27] Human intelligence (HUMINT) is defined as any information that can be gathered from human sources.

operations; the responsible for SIGINT[28] was the NSA; and for pictures and other IMINT[29] the responsible was the NGA.

Analysis was not primarily organized by problem or issue, but by agency. The Directorate of Intelligence of the CIA was first among equals, but the DIA was big too, and the much smaller INR tended to demonstrate its strength in interagency discussions. Each military service had its own intelligence arm, and the joint combatant commands also had their intelligence units.

The way in which collection and analysis were structured was logical during the cold war. On the collection side, with the Soviet Union and its allies target, the structure asked the stovepipes what could be added to their understanding of the target, and what puzzle pieces could be added to solving the Soviet puzzle.

On the analytic side too, the intelligence organizations' work was mainly focused on the Soviet Union. In that circumstance organizing by agency permitted a combination of competition, with analysts from different agencies looking at the same information from different perspectives, specialization and professional backgrounds. The organization by agency meant that all the analytic organizations, with exception of the CIA, worked for a set of consumers and for that reason could adapt their work according to the needs of those consumers. The final Cold War heredity was the product of the boundaries. Differently from the majority of partners, the United States had not created a domestic-intelligence service. To some degree, the FBI continued to perform the domestic-intelligence function. It was part of an FBI that primarily was a law enforcement organization that provoked the post-September 11 quips about trying to understand the FBI pre-September 11 through intelligence. Intelligence might have been important but certainly it was not central. Second, the function of the domestic-intelligence was limited by the boundary between law enforcement and intelligence, a "wall" that was extended inside the FBI too, and weakened the cooperation among the official of intelligence and law enforcement.

[28] The Intelligence Community refers to the collection and exploitation of signals transmitted from communication systems, radars, and weapon systems as signals intelligence (SIGINT)
[29] Imagery intelligence (IMINT) includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media

The institutions, conceptions and practices that were developed during the "Hot War" and the long following Cold War might have served the United States well enough then, even though that is a debated point.[30] Anyway, they set up the nation to fail on September 11, 2001, and they keep on setting it up to fail. The wrong combination is more visible in the campaign against terrorism. However, the heredity ran well beyond terrorism and non-state actors, and affected also how military power was designed and how its use was perceived.

It is important too highlight that this wrong combination heredity was not completely inflicted on the United States. "Those mismatches were also done in the name of civil liberties and privacy and were a sensible response to the threat the nation then faced."[31]

The price of the cooperation between the CIA and the FBI became very high on September 11, and brought the nation to rethink the set of organizational distinctions and procedural restraints that it developed during the Cold War. The country came, at the end, to a striking of the equilibrium between privacy and security. September 11 brought the nation to face a very different threat, one that forces a rethinking of the equilibrium, uncertain as the Cold War process. Moreover, the balance struck, combined organizational distinctions with constitutional protections and restraints on official discretion. Consequently, the rethinking involved how government organizations related to the Constitution, to one another and to the citizens of the country.

By the mid-1970s the communist threat on the home front had almost disappeared. In that context, the nation's first ever investigations of intelligence looked for abuses of the Americans' rights and found them, especially in a curious mixing of intelligence, counterintelligence and law enforcement at the FBI during J. Edgar Hoover's mandate as director. The justification and apparent target of these

---

[30] For a recent litany of failures, see Richard L. Russell, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right,* Cambridge, Cambridge University Press, 2007

[31] See Amy Zegard, *Flawed by Design: The Evolution of the CIA, JCS, and NSC,* Stanford CA, Stanford University Press, 1999. Her perspective analysis is exaggerated and deterministic. To be sure, the bureaucratic interests she emphasized played a role in how processes and institutions developed. Anyway, so too did the broader currents of domestic politics and national values.

"counterintelligence programs" was the operations of hostile foreign intelligence services and their possible engagement in protests against the Vietnam's war.[32]Anyway, the specific target of the majority of counterintelligence programs were American citizens in civil rights and antiwar groups. The domestic-intelligence activities of the FBI were suddenly restrained, and the "wall" that separated intelligence from law enforcement was becoming more and more high. A compromise between presidential discretion and civil liberties resulted in the 1978 passage of the FISA (Foreign Intelligence Surveillance Act) and the creation of the FISC (Foreign Intelligence Surveillance Court), a court that operated secretly in order to grant covert wiretapping and other surveillance authority for intelligence purposes.[33] Before the FISC, presidents had asserted the right of searches for national-security aims with no warrants at all, an assertion to which President George W. Bush returned after September 11.

The wall between intelligence and law enforcement had effects across both the domains, and the FISA made the divide clear. If the FBI or other officials sought wiretaps or other surveillance for criminal cases, they had to submit title III affidavits to federal courts, indicating the "probable cause" that the location or communication line being bugged had ever been or was being used to commit crimes. If, by contrast, the purpose of the surveillance was national security, with no reasonable case that a crime had yet been committed, then the chain of procedure was from the FBI to the Department of Justice to the FISC.[34]

It is difficult to convict espionage because the foreign power handling an American spy is hardly likely to cooperate. In such circumstances, most convictions take place when spies confess, which means that probable cause would be too high a standard even for criminal cases of espionage.

As long as the primary purpose of the FISA and the FISC was to sanction surveillance on foreign installations in the United States or on Americans suspected

---

[32] See *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate,* 94th Congress, 2nd Session, 1976; Book II, *Intelligence Activities and the Rights of Americans*; and Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans.*

[33] The Act is the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783

[34] Gregory F. Treverton, 2009, p. 53

of spying for foreign powers, they were relegated as Cold War. During the post September 11 debate about whether more could and should have been done to prevent the attacks, and also five years later, when it became known that President Bush had ordered the NSA to increase interceptions of communications in the wake of September 11, the FISA and domestic intelligence became well known. The reason why the administration did not use the FISA process to authorize the wiretaps was that the FISA process was too cumbersome; anyway,

> *the music behind the words was a return to the historical debate that presidents had an innate right to resort to warrantless surveillance when national security was at stake.*[35]

If, until September 11, the researches of the 1970s were the final act in hitting the Cold War balance between liberty and security, they stopped on a longer history of postwar institution building. Now, the rebalancing signifies not only the mixing of intelligence and law enforcement organizations and the refashioning of their culture, but it means also the rethinking of the basic class of threat and response. Law enforcement and intelligence are very different; they have different missions, operating codes and standards.

John Le Carré refers to intelligence as to "pure intelligence", describing it as oriented toward the future and toward policy; this means, "it tries to inform the making of policy."[36] Living in a storm of uncertainty, where the "truth" will never be known for sure, intelligence tries to understand new information in view of its existing understanding of complex situations. The Intelligence's officials want desperately to stay out of the string of evidence in order not to testify in court, this because intelligence struggles to protect methods and above all, sources. Protecting sources and methods is the main and most important activity of intelligence.

---

[35] The idea that the president, given his innate powers, could not be constrained by law during wartime is often called the "unitary executive theory." The argument, made often by Vice President Dick Cheney, had its intellectual godfather in John Yoo, The Berkeley law professor who served in the Justice Department's Office of Legal Counsel, where he wrote or contributed to a number of the memoranda about interrogation. See his *The Power of War and Peace: The Constitution and Foreign Affairs After 9/11,* Chicago, University of Chicago Press, 2005

[36] John le Carré, *The Night Manager,* New York, Knopf, 1993, p. 42.

Law enforcement, on the contrary, is oriented toward rather than forward response; that means after the fact. Its business is not policy but prosecution, and the method it uses is cases. Law enforcement struggles to put "bad guys" in prison. Law enforcement knows that if it is to make a case, it must be prepared to disclose something of it knows what it knows; this means that it is aware of the fact that it will face that choice.[37] Traditional law enforcement has no real history of analysis in the intelligence sense of the term; in effect, the meaning of the word intelligence is different for law enforcement, where it means "advice" to find and condemn criminals more than looking for models to frame future decisions. "Intelligence-led policing" rejects the reactive nature of law enforcement, trying instead to identify and manage emerging criminal problems. In summary, it tries to prevent the next crime and not just to prosecute the last one. However, it is primarily a collection strategy that highlights awareness of the local domain, in that it has much in common with the so-called "community policing".[38]

Cooperation between intelligence and law-enforcement was probably best in the Counterterrorism Center (CTC), under the DCI before the 2004 Act but mainly a CIA organization, and the limits even there were recommended by the handling of the terrorist watch list. As CTC was an intelligence organization, its mainly orientation was and still is abroad.

A second distinction, domestic versus foreign, emphasized the law enforcement-intelligence disconnect.

A third distinction is public versus private. During the Cold War, national security was a government – and, mainly, a federal government – monopoly.

If the complicated cooperation between the CIA and the FBI testifies the limited cooperation across foreign and domestic, other aspects of the September 11 failure faces the third main Cold War heredity: the mission and practices of FBI. The Bureau was mainly a law enforcement organization; nearly immediately after

[37] Gregory F. Treverton, 2009, p. 55.

[38] See, for example, David Weisburd and Anthony A. Braga (eds.), *Police Innovation: Contrasting Perspectives,* Cambridge, Cambridge University Press, 2006; Darric Milligan et al., *Intelligence – Led Policing Technology for State and Local Law Enforcement Agencies,* Bedford MA, Mitretek Corporation, MTR-2006-016, 2006; and Jerry H. Ratcliffe, "Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice", *Policing and Society, 12,* 1 (2002), 53-66.

September 11, Director Robert Mueller began a profound change in the mission of the FBI to prevention and intelligence.

Director of the FBI Robert Mueller

That Bureau was and is ruled by special agents, and naturally, those agents were attracted to where there were criminals to be captured. As a consequence, the FBI viewed the world through the lens of the case and case file. If information was not significant to making a case, it was trivial. For this reason, the post September 11 investigations were full of reports of terrorism training handbooks and similar materials that went un-translated for years because they were not relevant for a specific case.

The Moussaoui misadventure describes some of the characteristics of the FBI organizational culture, although it was not brought to an end in the center of the organization, law enforcement. Rather, it was in counterterrorism, which was before September 11 not surely "an area where there were many collars to be made."[39] On July 10, 2001 an FBI special agent in the Phoenix field office sent an electronic communication to the FBI headquarters and to the New York field office.[40] The electronic communication advised about potential risks from Al-Qaeda affiliated individuals that were training at U.S. flight schools. To the Usama Bin Laden Unit (UBLU) and the Radical Fundamentalist Unit (RFU) within the Bureau's

[39] Gregory F. Treverton, 2009, p. 62.
[40] This episode is discussed in the joint congressional investigation *Final Report*, and in Shelby's *Additional Views*, p.18.

counterterrorist organization, a memorandum was sent, but the headquarters personnel decided that no follow-up was needed. Surprisingly no managers took part in this decision or saw the memorandum before September 11 attacks. The CIA came to know the Phoenix special agent's preoccupation about flight schools, but it gave no comments in spite of the information possessed by the CIA about the interest of terrorists in the use of aircrafts as weapons.

Neither did the FBI officials that saw the Phoenix electronic communication at headquarters connected that preoccupations with the information that the FBI already possessed about the interest of terrorists in getting training at U.S. flight schools. At the beginning, the content of the Phoenix Memo was not made public, but it is strange that so little was made, particularly because it called the attention to certain information already in possession of the FBI, suggesting a specific explanation to be alarmed about a particular foreign student attending an aviation university in the United States.[41] The case of Moussaoui suggested that the FBI and the Justice Department might have set the bar too high, at least before September 11. In that event, FBI and headquarters lawyers informed by the agent that dealt with the case, believed that there was not enough evidence for a FISA search.[42] The Moussaoui case can be seen as a testament to rough procedures, poor information technology, extreme caution or simple ignorance about complicated points of the law, tension between FBI offices and headquarters, or as all cases combined.

[41] A heavily redacted version of the memorandum is available at: http://www.investigativeproject.org/documents/case_docs/1171.pdf

[42] This account derives from *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures* (February 2003), pp. 14ff, available at: http://www.fas.org/irp/congress/2003_rpt/fisa.html

1.9 TERRORISM AND PREEMPTIVE PROSECUTION

From many points of view, counterterrorism responds to the two classic Bureau missions, which are counterintelligence and criminal law enforcement, reflected in the work of the Criminal Investigative Division (CID)[43] and the Counterintelligence Division (CD)[44]. Consider that CID informants, for example, are themselves criminals who will probably commit unauthorized crimes. That's why we can say that countering terrorism has much in common with operations against organized crime and drug traffickers. The intelligence responsibility puts a premium on unraveling networks, which often include countries and continents. The major difference is that criminals want to live for their cause and not to die for it; they want to live in order to steal another day.

Terrorists, instead, are ready to die for their cause. This is what drives the task of intelligence back to prevention or preemption. Another difference, then, is between the fight against terrorists and against crime: due to the fact that potential terrorists must be stopped before they strike, the decision to organize the operation has to be taken earlier. Anyway, terrorists cannot be permitted to strike and so they need to be found and stopped before they act. Combating them is really risky, and it often means relying on unreliable informants to infiltrate insular communities and arresting before anything similar to a terrorist attack happens. Sometimes the process ends with a prosecution, but as often as not it ends without a conviction. Consider that since September 11 there is a record of U.S. convictions of terrorists. Even though the process is an unsatisfying and confusing ordeal, it is sometimes the best that can be done. Prosecution may not be the point, stopping terrorist secret plans is. The risk

[43] *The Criminal Investigative Division (CID) is the FBI's largest operational division, with 4,800 field special agents, 300 intelligence analysts, and 520 Headquarters employees addressing an array of sophisticated and increasingly globalized criminal threats. Having served as a foundational strength of the FBI for nearly a century when the events of 9/11 took place, CID has confronted significant challenges to its traditional business model as the FBI has grown to meet the national security threats facing the U.S.*

[44] The mission of the Counterterrorism Division is to help the United States to prevent acts of terrorism against the U.S. and U.S. targets

is that innocent people will go to prison on poor evidence or, on the contrary, judges will become so suspicious about informants that they will free guilty people. In the long term, the risk is that hearsays of entrapment will become so strong that they will undermine relations between the FBI and other government agencies or potential allies. The question will still be

> *how much the intelligence-agency model for the FBI will need to be adapted to an organization that will keep a powerful law enforcement past and continuing mission and that will be moving toward more emphasis on a counterterrorism mission that passes through law enforcement and intelligence.*[45]

With respect to the old mission, the new one is much more preemptive and directed on public safety by looking ahead to consequences and acting accordingly.

Agents are a "band of brothers and sisters" that easily share information between them. However, before September 11, FBI agents were not distinguished by their willingness to share outside the band. The Bureau led state and local police officers to work with it.

The culture is strong and powerful, and operates in the interest of the public. Changing the culture is a difficult and slow process. The FBI culture appreciated action and favored agents on the street over technology. It was and still is a culture of law enforcement that puts a premium on sharing information and not on keeping them secret. The spirit of the organization is that they can do it, and this spirit makes the gap between headquarters and the field awesome. The question for the future is how much this heredity needs to be changed and effectively how much it can be changed.

The events of September 11, 2001, stated clearly that international terrorism is a serious national security threat and induced a major reevaluation of cooperation and information exchange among all principal law enforcement and intelligence agencies. Following the attacks, the Congress began to remove barriers among the agencies, and, above all, it tried to ensure that information available from sources of law enforcement, would be made accessible to intelligence agencies. Seeking the

[45] Gregory F. Treverton, 2009, p. 73.

Al-Qaeda network, all information had to be used to support a multi-phased attack by military and intelligence agencies and by law enforcement.

Most observers believe that the destruction of the Al-Qaeda network in Afghanistan will not lead to the end of international terrorism. Striking them back will need intelligence and law enforcement agencies to collaborate. "It is believed that the two efforts can't be simply conflated, and the most important constitutional differences will remain."[46]

> *Today, there is no clear primacy for either the law enforcement or intelligence communities in the realms of international terrorism, narcotics, proliferation (as well as, in some cases, counterintelligence). Still, the law enforcement and intelligence communities remain designed and operated in fundamentally dissimilar manners, retaining different legal authorities, internal modes of organization, and governing paradigms.*[47]

[46] A. Richard, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS Report for Congress, Updated December 3, 2001, p. 32

[47] Jonathan M. Fredman, *Intelligence, Law Enforcement, and the Prosecution Team,* Yale Law and Policy Review, 1998, Vol. 16, No. 2, pp.336-337

CHAPTER 2

THE NEED FOR CHANGE

2.1 INTRODUCTION

The boundaries that supported democratic nations quite well during the Cold war by protecting the privacy of citizens, in an age of terror, instead, led those nations to fail. Terrorists respected none of the boundaries. Terrorists were not "over there," they were both here and there. By the mid-2000s, for example, the terrorist threat to Britain was mainly "domestic". For the United States, on the contrary, the problem was still mainly "over there".

The terrorists' targets were private citizens rather than armies, and, as a result, the war to terrorism not only encouraged the threat but also dislocated it. Terrorists could not be dealt with intelligence or law enforcement problems but they had to be treated as both.

If organizing intelligence might have made a certain sense during the Cold War, it cannot be the right way to arrange it now.

> *If the terrorist target is more of a mystery than a puzzle, then the implicit competition of the Cold War among the INTs for puzzle pieces needs to give priority to explicit cooperation across those INTs in framing the mysteries.*[48]

Moreover, now there are not only more targets, but also more information and more consumers.

The 2004 Act began a reshaping of intelligence. It proposed the creation of national intelligence centers under the DNI's authority, organized around missions or topics. The national intelligence centers, following the example of the National Counterterrorism Center (NCTC), would both deploy and use the technology,

[48] Gregory F. Treverton, 2009, pp. 75-76.

information and staff resources of the existing agencies. The centers would be the intelligence's version of the "unified combatant commands", with the task of looking to the agencies in order to acquire the technological systems, train people and carry out the operations planned by the centers.

2.2 HITTING THE "WALL"

The effect of all the Cold War boundaries was clearly visible in the run-up to September 11.[49] By the spring of 2000, two of the hijackers, Nawaf al-Hazmi and Khalid al-Mihdhar, were living under their real names in San Diego, and Nawaf even applied for a new visa. The Immigration and Naturalization Service (INS) had no reason to be worried because the CIA had rejected the two names from TIPOFF, the terrorist watch list. The FBI neither had any reason to look for them, and the reason was that the last it knew from the CIA was that the two were overseas. The Federal Aviation Administration (FAA) was not told to be on alert for them, maybe because it was not in the law enforcement business.

According to the joint Senate-House investigation of September 11, the CIA's procedures for the transmission of information to other agencies – FBI, NSA, INS and State – of suspected terrorists were both limited and imprecise.[50] The CIA should have notified at least the FBI and the NSA of all people suspected of being terrorists. In fact, it seems that the CIA put people on the watch list if it had information that they were near to travel to the United States. After September 11, the number of the names of the watch list increased immensely.

The difficult connections between the CIA and the FBI were graphically illustrated by their misleads over the Al-Qaeda affiliated terrorists. The story of what the two agencies told each other and when, was told in the series of investigations of September 11 tragedy.

The FBI affirmed that in late August 2001 it learned that Mihdhar and Hazmi were al Qaeda operatives and that they had traveled to the United States in January 2000. In August 2001, the FBI also discovered that Mihdhar had entered the United States on July 4, 2001, presumably for a month-long stay.

---

[49] The most complete account of these events is the 9/11 Commission Report, formally the "National Commission on Terrorist Attacks Upon the United States," *The 9/11 Commission Report,* Washington, DC, 2004, available at: http://www.9-11commission.gov/report/

[50] The findings of the joint House Senate investigation of September 11 sketched the basic story. It is *Final Report,* Part I, the Joint Inquiry, December 10, 2002. A complete account is contained in Senator Richard Shelby's long supplementary document, *September 11 and the Imperative of Reform in the Intelligence Community, Additional Views,* December 10, 2002

In late August, the FBI began an investigation in order to determine whether Mihdhar was still in the country and find him. The FBI was still looking for him at the time of the September 11 attacks. No evidence was found indicating that the FBI or any other member of the Intelligence Community had specific intelligence regarding the September 11 plot.

From the late 1999 and till September 11, 2001, five occasions were found where the FBI could have either learned of intelligence information about Mihdhar and Hazmi; could have learned of additional intelligence information about them; or could have developed additional information about their location and terrorist connections.

These five occasions were:

- Mihdhar's travel in early January 2000 to Kuala Lumpur, Malaysia, where he met other Al-Qaeda operatives. Intelligence information developed by the CIA in early 2000 showed that he was a suspected Al-Qaeda operative. The CIA discovered also that Hazmi had traveled to Los Angeles in January 2000;
- Mihdhar and Hazmi's travel in late January 2000 to Los Angeles and the following move to San Diego, where they associated with an ex-subject of an FBI investigation and also lived with a longtime FBI asset; in late December 2000 and January 2001, a reliable joint FBI/CIA source gave information related to the FBI's investigation on the U.S. Cole's attack;
- In the summer of 2001, the FBI and the CIA had different interactions regarding the FBI's investigation of the Cole attack. These interactions touched on the participants in the January 2000 Malaysia meetings and on information of the CIA about such meetings;
- In August 2001, the FBI learned that Mihdhar had entered the United States on July 4 and began looking for him in September 2001. It also learned that the purported organizer of the Cole attack had met with Mihdhar and Hazmi in the Malaysia meetings. The FBI did not manage to locate him before the September 11 attacks.[51]

[51] See *A review of the FBI's Handling of Intelligence Information Related to September 11 Attacks*, pp. 223 – 224.This report is a redacted and unclassified version of the full report that the Office of the Inspector General (OIG) completed in July 2004 and provided at that time to

In spite of these continuous discussions and opportunities for the FBI to learn about and focus on Mihdhar and Hazmi, it was not made aware of and so did not connect important details about them until late August 2001, a very short time before their participation in the terrorist attacks. In August too, the FBI's search for the two terrorists was not given any urgency or priority.

As a source told to the New Yorker writer Joe Klein, before September 11, the "Standard FBI line" was that "Osama Bin Laden wasn't a serious domestic security threat", maybe because his previous attacks had been abroad and not at home.[52]

the Federal Bureau of Investigation (FBI), the Department Of Justice, the Congress, the Central Intelligence Agency, the National Security Agency, and the National Commission on Terrorist Attacks Upon the United States. The OIG's full report is classified at the Top Secret/SCI level

[52] J. Klein, *Closework: Why We Couldn't See What Was Right in Front of Us,* The New Yorker, October 1, 2001, pp. 44-9

2.3 FIRST STEPS AT REFORM: THE 9/11 COMMISSION'S REPORT

In an unusual way, the 9/11 Commission brought the reshaping of American intelligence into a new territory. Its report was dramatic and its main recommendations were the reshaping of the U.S. intelligence organization and also a change in the way it does business. The 9/11 Commission, strangely, instead of reporting and then disappearing as always happens, stayed around, inciting the Bush administration and the Congress itself to make something happen.

Because the 9/11 victims' families were not about to be ignored, they added political influence to the Commission. Thanks to them the Commission was established, and the families, as well as fighting hard for public hearings and for the access to President Bush by the Commission, helped with their influence after the report was set free.

Between the emanation of the 9/11 Commission's report and the enactment of the Intelligence Reform and Terrorism Prevention Act of 2004, there was no continuity in the public debate over the merits of recommendations.

The tale of the commission about how the United States were surprised by the 9/11 attacks could not be otherwise. In retrospect it is easy to discover missed opportunities that would have prevented the attacks and come to a conclusion that the failure to prevent them

> *was the result not of bad luck, the enemy's skill and ingenuity, the inevitability that some surprise attacks will succeed, the personal failings of individuals, or the difficulty of defending against suicide attacks or protecting a well-night infinite range of potential targets, but rather of systematic failures in the nations intelligence and security apparatus.*[53]

The report's narrative demonstrates the political, psychological and operational difficulty in taking effective action to prevent a type of attack never occurred before. After the 9/11 attacks, measures were taken that have at any rate

[53] Richard A. Posner, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11,* Rowman & Littlefield Publishers, Inc., 2005, pp. 19-20

postponed the recurrence. Before 9/11, instead, even though the government knew that Al-Qaeda had attacked U.S. and would try to do it again, the idea that it would do so infiltrating operatives into the United States to learn to fly commercial aircraft and then crushing them into buildings, killing in this way thousands of American people in few minutes, was so dreadful that wasn't supposed to be considered possible.

A few months before the attacks the director of the Defense Department's Defense Threat Reduction Agency wrote:

> *We have, in fact, solved a terrorist problem in the last twenty-five years. We have solved it so successfully that we have forgotten about it; and that is a treat. The problem was aircraft hijacking and bombing. We solved that problem…. The system is not perfect, but it is good enough…. We have pretty much nailed this thing.*[54]

In such opinion's climate, efforts to increase airline security would have seemed unnecessary but would also have been rejected because of their costs. The problem then, is not only that people find it difficult to take risks that have never materialized in a serious way, but also that the government cannot examine all possible disasters and take expensive decisions to prevent each of them.

With reference to the FAA, the 9/11 Commission observed that

> *Historically, decisive security action took place only after a disaster had occurred or a specific plot had been discovered.*[55]

The 1993 bombing of the World Trade Center[56] brought many safety improvements in the Twin Towers that reduced the toll from the 9/11 attacks.

---

[54] Jay Davis, *Epilogue: A Twenty-First Century Terrorism Agenda for the United States,* in *The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors pp. 269-275* (James M. Smith and William C. Thomas eds., 2001)

[55] The 9/11 Commission Report, 2004, p. 83

[56] On February 26, 1993, a terrorist bomb exploded in a parking garage of the World Trade Center in New York City, leaving a crater 60 feet wide and causing the collapse of several steel-reinforced concrete floors in the vicinity of the blast. Although the terrorist bomb failed to critically damage the main structure of the skyscrapers, six people were killed and more

The 9/11 commission's report establishes that "the terrorists exploited deep institutional failings within our government".[57] As far as the statement concerns a lack of coordination among people and agencies that could have prevented or mitigated or responded to the attacks, it is defensible, but as soon as it concerns the structure of the intelligence system, it is not. In 1996 the U.S. intelligence was aware that Osama Bin Laden was a dangerous enemy for the United States.[58]

Osama Bin Laden at a news conference in Afghanistan in 1998

President Clinton and Samuel Berger, the national security adviser, became so worried that Clinton decided to visit Pakistan in order to establish its cooperation against Bin Laden. A lot of measures were considered in order to capture or kill Bin Laden, but no one worked.

The idea of an invasion of Afghanistan to prevent future attacks was considered, but President Bush rejected it for diplomatic reasons. The 9/11 Commission's report underlines the determination of President Bush to resolve the

---

than 1,000 were injured. For more detailed facts see *1993 Trade Center Bombing, available at* http://www.fbi.gov/news/stories/2008/february/tradebom_022608

[57] The 9/11 Commission Report, 2004, p. 265

[58] See Michael Scheuer, *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam, and the Future of America*, 2002

situation and destruct definitely Al-Qaeda. The President recalled the attention saying:

> *I'm tired of swatting at flies. I'm tired of playing defense. I want to play offense. I want to take the fight to the terrorists.*[59]

Four years after Bush's taking of office, Bin Laden was still at large and Al-Qaeda had not been destroyed.

Till the 9/11 Commission's report appeared, the sensation was that the failure to prevent the attacks was connected to the failure to integrate all pieces of information possessed by security services about Bin Laden, Al-Qaeda and Islamist terrorism at large. Even though all pieces would have been connected, there would have been only a possibility to prevent the attacks. Only in August 2011 the most important pieces were obtained, and it was too late to connect the dots in time to impede the plot.

When the narrative part of the commission's report ends, what the reader asks himself is: Which is the result of the Commission's Report? How can the nation be protected against international terrorism?

What emerges is that there has not been a real reorganization of the intelligence system:

The main buildings should have detailed evacuation plans and resources for the large-scale response should be increased; customs officials should be informed of modified documents of Muslims that enters in the U.S. and borders should be made less permeable with the institution of biometric and incoming freight screenings, in order to create a serious database of suspicious characters; cockpit doors should be secured and airline passengers and luggage carefully screened; legal and bureaucratic barriers for the sharing of information between the CIA and the FBI, and, within the FBI itself, between criminal investigators and intelligence officers, should be eliminated; major effort should be made to penetrate foreign terrorist groups; more Americans should be trained in languages used in the Muslim world; federal agents working for the "war on drugs" should be reassigned

[59] The 9/11 Commission Report, 2004, p. 202

to the war on international terrorism, where their competence could be employed for a major benefit of the nation; cooperation among different agencies, which role is to prevent and respond to terrorist attacks, should be improved; and finally, a separate security agency should be created, based on the model of England's MI5 rather than leave only federal responsibility for domestic security to the FBI.

Of all the agencies involved in intelligence and counterterrorism, the FBI is the worst described in the commission's report. After 9/11, the Bureau, under the new director Robert Mueller, promised to do better. Doubts were not about its intelligence, commitment, energy and clarity of aim, but rather whether its efforts would have been successful. "Two years passed, after 9/11 for the Bureau to dream up a plan to reform its counterterrorism program."[60] But the truth is that even three years after realizing the inadequacy of its information technology for intelligence purposes, the Bureau had still not success.

Some of the reforms listed have been adopted and implemented. There have been improvements in aircraft safety and border control. Legislation may have been unnecessary because before 9/11 the FBI and the CIA overstated the degree to which they were allowed to share information, and the FBI overstated the degree to which its criminal investigators and intelligence officers were allowed to share information between them. The CIA's main concern was the fear of information being revealed in court proceedings; the Bureau's main preoccupation was about transgressing legal limitations on the revelation of testimony before grand juries. Efforts were made to increase linguistic and cultural competence of the intelligence services. The 9/11 experiences brought to various cooperation agreements among different agencies worried about public safety. With Director Mueller, the Bureau became more active in the penetration of extremist groups and transferred many agents from the drug war to the terrorism war. Strangely, the better planning for the evacuation of buildings attacked seems to have slowed down. As the U.S. struggle against Islamist terrorism is impeded by ignorance of languages, peoples, culture,

[60] Laurie E. Ekstrand, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities,* U.S. General Accounting Office GAO-94-578T, 2004, p. 6

politics and history of the Muslim world, their ability to devise effective antiterrorists methods suffers from a rejection to consider foreign models.

Even if all the measures mentioned were fully implemented, the probability of another terrorist attack would not be reduced. The commission's report establishes that the focus of the antiterrorist strategy should not be

> *"just terrorism, some generic evil. This vagueness blurs the strategy. The catastrophic threat at this moment in history is more specific.it is the threat posed by Islamist terrorism."*[61]

Describing the political and psychological difficulty of taking seriously threats that have never materialized in the past, the recommendations of the commission's report are directed toward preventing what is already rather than unlikely. Very few sentences are dedicated to the possibility of nuclear terrorism and terrorist threats to other means of transport besides air, and the other range of potential terrorist threats is quite ignored.

However, many specific recommendations of the commission's report are sensible, like the fact that American citizens should be required to carry biometric passports. An attractive recommendation is the reduction of the number of congressional committees that missed responsibilities for intelligence. A reason for such reduction was that with so many committees exerting oversight, senior intelligence and national security officials spent too much of their time making tests. Another reason is that if there were many masters to answer to, the scope for action and initiative would be limited because of the different view of each one.

An objection to consolidation deals with the large classified portion of the intelligence budget. Actually most of that portion is hided in the defense budget and appropriated by the defense appropriation subcommittees. If the intelligence budget were separated from the military one, both the size of the overall budget and the appropriations for specific programs would be more difficult to hide.

[61] The 9/11 Commission Report, 2004, p.362

2.3.1 THE CREATION OF THE DIRECTOR OF NATIONAL INTELLIGENCE

The 9/11 commission's main proposal was the creation of a new position, the Director of National Intelligence. The position of the Director of Central Intelligence (DCI) would be abolished and there would have been no more a single official both as head of the CIA and as president of the entire intelligence community. The DNI would have become the chief executive officer of the intelligence community. His main assignment would have been to overcome the reluctance of the different intelligence agencies to share information regarding terrorist activities, and to cooperate.

John Dimitri Negroponte named in 2005 the first ever Director of National Intelligence

First of all, the National Intelligence Director role was the supervision of national intelligence centers in order to let them provide all-source analysis and plan intelligence operations for the government on the main problems.

One problem, for example, is counterterrorism. It was believed that the center had to be the intelligence organization inside the National Counterterrorism Center.

Other national intelligence centers were to be housed in whatever agency or department best appropriated for them. The DNI had to consider the DCI's role as the principal intelligence adviser to the president.

> *We hope the president will come to look directly to the directors of the national intelligence centers to provide all-source analysis in their areas of responsibility, balancing the advice of these intelligence chiefs against the contrasting viewpoints that may be offered by department heads at State, Defense, Homeland Security, Justice, and other agencies.*[62]

Second, the DNI had to manage the national intelligence program and supervise the component agencies of the intelligence community. He had to propose a unified budget for national intelligence that would have reflected priorities chosen by the National Security Council.

> *He or she would receive an appropriation for national intelligence and apportion the funds to the appropriate agencies, in line with that budget, and with authority to reprogram funds among the national intelligence agencies to meet any new priority.*[63]

The DNI had to manage the national effort helped by the foreign intelligence, the defense intelligence and the homeland intelligence, which would also have had a key position in one of the component agencies. Other agencies of the intelligence community had to coordinate their work within each of these three areas. These three areas had also the role to acquire systems, train people, and execute operations planned by the national intelligence centers. Combatant commanders had to report to the secretary of defense, the directors of the national intelligence centers as well as to the DNI. The department was responsible of the Defense Department's military intelligence programs.

> *The National Intelligence Director would set personnel policies to establish standards for education and training and facilitate assignments at the national intelligence centers and across agency lines. The National Intelligence Director also would set information sharing and information*

[62] Ibid, p. 411
[63] Ibid, p. 412

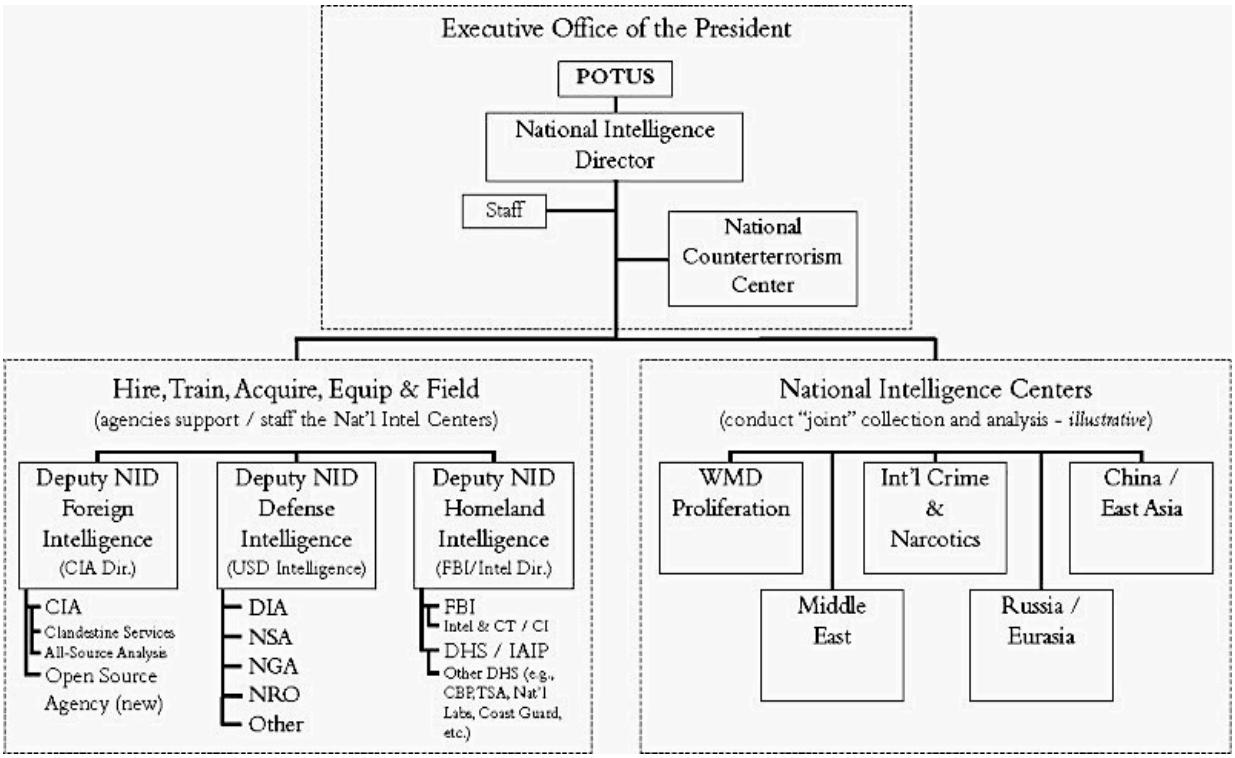
technology policies to maximize data sharing, as well as policies to protect the security of information.[64]

The DNI had to participate in a National Security Council executive committee in order to solve differences in priorities among the agencies; in this way, the main debates would have been submitted to the president for decision.

The DNI, located in the Executive Office of the President, and confirmed by the Senate and testifying before Congress, had a staff of several hundred people that assisted him, taking the place of the existing community management offices present at the CIA.

The National Intelligence Director still provides a service function in the management of the whole community, after all the DNI role should also be to support the consumers of national intelligence.

Unity of Effort in Managing Intelligence



[64] Ibid, p. 414

Some disadvantages would be found if the position of the DNI was separated from the job of heading the CIA. For example, the DNI would not have headed a major agency of his own and could have had a weaker base of support. But the 9/11 Commission's report explains that such disadvantages are outweighed by many other considerations: the DNI should be able to directly supervise intelligence collection inside the U.S.. However, law and custom has advised not to give such a plain domestic role to the head of the CIA; the CIA would be one among numerous claimants for funds in setting national priorities. The DNI had neither to be one of the advocates nor the judge of them all; covert operations, which tend to be extremely tactical, would have required close attention. The DNI had to rely on the relevant joint mission center in order to supervise such details, so that he would have helped to coordinate closely with the White House. The CIA had to be able to concentrate on building the capabilities to carry out such operations and on providing the personnel who would direct and execute such operations in the field; the rebuilding of "the analytic and human intelligence collection capabilities of the CIA should be a full-time effort, and the director of the CIA should focus on extending its comparative advantages."[65]

The CIA Director had to rebuild the CIA's capabilities of analysis; transform the clandestine service with the building of its human intelligence capabilities; develop a stronger language program; renew emphasis on the recruitment of diversity among operations officers; ensure a strong relationship between human source collection and signals collection at the operational level; and emphasize a better balance between unilateral and liaison operations. The CIA had to keep responsibility for directing and executing clandestine and covert operations. Before 9/11, the CIA instead of investing on the development of a robust capability to conduct paramilitary operations with U.S. personnel relied on proxies organized by CIA operatives. The results were not satisfactory.

The United States should have concentrated responsibility and necessary legal authorities in one entity, because they were not able to build "two separate

[65] The 9/11 Commission Report, 2004, p. 415

capabilities for carrying out secret military operations, secretly operating standoff missiles, and secretly training foreign military or paramilitary forces."[66]

Finally, the 9/11 Commission's Report recommended that to combat the secrecy and complexity described, the total amount of money appropriated for national intelligence and to its component agencies had no longer to be a secret.

> Congress should pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work.[67]

[66] Ibid.
[67] Ibid, p. 416

2.3.2 THE CREATION OF THE NATIONAL COUNTERTERRORISM CENTER

In July 2004, the 9/11 Commission noted the existence of a great number of centers in different parts of the government and so decided to call for the establishment of a National Counterterrorism Center (NCTC). The NCTC was built on the basis of the Terrorist Threat Integration Center (TTIC) but had the responsibility for joint planning for responding to terrorist plots and to assess intelligence from all sources. According to the 9/11 Commission,

> *the NCTC would complete all-source information on terrorism but also start to plan counterterrorism activities, assigning operational responsibilities to lead agencies throughout the Government.*[68]

The National Counterterrorism Center in Virginia

The NCTC was considered the primary organization of the Federal Government for the analysis and integration of all intelligence possessed or

[68] Richard A. Best Jr., *The National Counterterrorism Center (NCTC)-Responsibilities and Potential Congressional Concerns,* December 19, 2011, p. 3

acquired concerning terrorism or counterterrorism. The NCTC would not just have the analytical responsibilities possessed by the TTIC; it would also assign operational responsibilities to lead agencies for counterterrorism activities, but the NCTC would not direct the execution of operations. The Director of the NCTC would be appointed by the president and confirmed by the Senate. The DNI role is to supervise the NCTC's operations and budget, while the director has to report to the DNI on intelligence and intelligence operations. However, the NCTC director "reports to the president with regard to counterterrorism operations other than those in intelligence".[69] Such dual reporting would be necessary if the NCTC was to play a real role in planning the counterterrorism operations of the government. In this way, however, the risk is a further weakening of the DNI by the separation of the loyalty of a principal subordinate.

Some members of the Congress, however, continued being worried about the status of NCTC, the probability that

> *Congress would have no role in the appointment of its leadership, and the possibility that an interagency entity might not be responsive to congressional oversight committees.*[70]

In a positive sense, the conception of the NCTC pivots the idea that in an age of terror, the mission of the counterterrorism is rich in intelligence, so the planning needs to be driven by intelligence. Generally, the federal government achieves interagency coordination by designating a lead agency or passing the responsibility of coordination to the White House.

The Intelligence Reform and Terrorism Prevention Act of December 2004 (P.L. 108- 458) put into effect many of the 9/11 Commission's recommendations.

> *The position of the NCTC Director is unusual, if not unique, in government; he reports to the DNI for analyzing and integrating information pertaining to terrorism (except domestic terrorism), for NCTC budget and programs; for planning and progress of joint counterterrorism operations (other than intelligence operations) he reports directly to the President. In practice, the*

[69] Gregory F. Treverton, 2009, p. 91
[70] The National Counterterrorism Center, 2011, p. 3

NCTC Director works through the National Security Council and its staff in the White House.[71]

[71] Ibid., p. 4

2.3.3 THE CREATION OF NATIONAL INTELLIGENCE CENTERS

With the NCTC prototype, the creation of national intelligence centers under the DNI authority and their organization around issues was the most profound change proposed by the 9/11 Commission, in the way intelligence does its business.

The centers were supposed to deploy and use the technology, information and staff resources of the existing agencies. In the 9/11 Commission's vision, there had to be the unified commands

> *looking to the agencies to acquire the technological systems, train the people, and execute the operations planned by the national intelligence centers. They were to bring together analysts, information collectors, and operations specialists around problems or issues, not collection sources or agencies.*[72]

The 2004 bill permitted the creation of the centers. At present, many centers bring together officers from a number of intelligence agencies. The proposal of the 9/11 Commission would have intensified such connections with the establishment of the national intelligence centers as the primary way in which the intelligence community does its work. The centers that had been created earlier were and still are the creatures of the agencies, but in the proposal of the 9/11 Commission, the agencies were supposed to become their supporters.

There were and will continue to be preoccupation about such organization by centers, and what is worst is that the first DNI's did not encourage the idea of such organization. The first preoccupation is that there is no real infrastructure to support this idea, in personnel or technology. Second is the fact that the existing agencies argue that the centers would be inclined toward focusing on current intelligence and would therefore tend to produce worst-case analyses, and this because they are the primary producers of intelligence.

[72] Gregory F. Treverton, 2009, p. 92

Based on the military's unified commands' experience, those are considered serious objections, even though at this point, the similarity between military commands and the centers begins to collapse. The military commands tend to have a short-time sight and to worry about the worst: this is understandable because if a war broke out now they would have to fight it. Similarly, the centers would be the first to be accused if crises develop without warning and their plans would be the first to be subjected if remedies fail.

2.4 THE RESPONSE OF THE CONGRESS

In spite of their numerous flaws, the organizational recommendations in the 9/11 Commission's report, led to an immediate and positive congressional response. The important thing is to trace the path that starts from the commission's report to the final legislative action, in order to see how that action affected the commission's recommendations.

Senator Pat Roberts made one of the first congressional responses.[73] His proposal intended to improve the commission's proposals. His idea was to break the CIA into three parts: collection, analysis and science/technology. His idea was to obtain a new agency from the Defense Intelligence Agency (DIA) and to place all the intelligence agencies under the DNI. Intelligence agencies are highly different among them and, like the commission itself, Senator Roberts seems not to have considered whether it would be sensate to place all agencies under a single official.

On September 23, 2004, Senator Susan Collins introduced a bill (S. 2845) with the intention to enact the 9/11 Commission's main recommendations. Senate Majority Leader Frist, designated her committee to address intelligence reform legislation through the Senate. As neither Collins nor Frist were intelligence's experts, "the choice of the Governmental Affairs Committee to shepherd the reform legislation through the Senate was therefore an odd one".[74]

By bypassing the Senate Select Intelligence Committee and the Senate Committee on the Armed Forces, the Majority Leader's decision removed a dangerous obstacle. The Senate, in effect, passed the bill only two weeks after its introduction. Another bill, supported by the Speaker of the House, passed the House in two weeks. Both bills were referred to a conference committee to level their differences.

The Senate version went very close to the 9/11 Commission's recommendations. The bill

[73] 9/11 National Security Protection Act, available at: http://www.fas.org/irp/congress/2004_cr/roberts-911nspa.pdf
[74] Posner, 2005, p. 53

> *eliminated the requirement of "dual-hatted" deputies to the Director of National Intelligence (the Undersecretary of Defense for Intelligence and the intelligence chief either of the FBI or of the Department of Homeland Security); dropped the proposal to transfer the CIA's paramilitary division to the Defense Department; established an Office of Alternative Assessments to serve a "devil's advocate" role in the intelligence community; required every FBI agent to have some training in intelligence (a Band-Aid solution if ever there was one); created a civil liberties watchdog board; but left the existing system of multi-committee congressional oversight intact.*[75]

The bill of the House (H.R. 10), instead, reduced the authority of the DNI, and in particular his authority over the budget of the intelligence's Department of Defense. An important way in which the House Bill differed from the Senate bill was that it added a number of provisions in order to strengthen domestic law enforcement rather than restructuring the intelligence system. Both bills included a number of other recommendations of the 9/11 Commission, but the House bill added provisions that went beyond the Commission's proposals and what the Senate included in its bill. Such provisions imposed new restrictions on the rights of asylum seekers and other type of immigrants.

The only criticism the 9/11 Commission's organizational recommendations received during the congressional considerations of the bills came from defense officials and their congressional supporters. It was thought that the DNI would have interfered in some way with the transmission of tactical intelligence from military spy satellites to troops in the field, causing danger to the troops.

The real concern of the Department, was that the DNI would use his authority and budgetary to modify the balance of military and antiterrorist intelligence-gathering efforts in favor of the last one. The Defense Department would not like its intelligence agencies concentrated on strategic intelligence to be deviated from gathering intelligence about military capabilities and foreign states' intentions to gathering intelligence about terrorists.

[75] Ibid.

George W. Bush

President Bush was trapped in the support of the 9/11 Commission's proposals by the confluence of many factors, so he could not be responsive to this concern. First, within days of the issuance of the commission's report, the Democratic Presidential nominee, at that time Senator Kerry, promoted all its recommendations without reservations. After the promotion of the commission's recommendations, President Bush could hardly withdraw it after winning the election. Second, as the Republicans unexpectedly gained seats in the Senate and in the House of Representatives in the election, and with them the control of the entire Congress, the failure of Bush to obtain promotion of the commission's recommendations would have be seen as a weakness and as his inability to control his own party. Third, it was a failure by the media to submit the commission's recommendations or the legislative follow-up to continuous, critical scrutiny.

> *"The commission's bipartisan composition, its unanimity, its sentimental alliance with the families of the victims of the 9/11 attacks, the rhetorical adroitness and sheer heft of its report, journalists' aversion to complex and abstract issues of public policy, the curious lack of interest in the subject by the media-adept public intellectuals, the natural reticence of intelligence officers, the unpopularity of the intelligence agencies, a sense on the part of a number of members of Congress of both parties that the President*

> *had actually done little to strengthen the intelligence system in the wake of 9/11, the timing of the release of the commission's report in the midst of the Presidential election campaign, and its enduring endorsement by both Presidential candidates,"*[76]

paralyzed most public and private criticism and conferred holy status to the report and its recommendations.

The media portrayed the legislative dispute as one of territorial wars and politics: the fight of the Department of Defense to keep its territory and the need of the President to prove his control over the Congress. It can be thought that the liberal media supported the legislation for a reflex enthusiasm for reform and aversion to the CIA. The conservative media supported it because they favored the strengthening of national security.

A fourth possibility is that the President endured any doubt about the organizational provisions of the new act because he thought them being irrelevant in operation.

The President might have felt that the structural provisions of the Intelligence Reform Act did little more than deleting the National Security Act of 1947 section that made the DCI also the head of the CIA. With that deletion, the President could have released the time of the director for the exercise of new powers by the appointment of a different person to head the CIA.

Such amendment wasn't necessary for the President to free the DCI from most of his day-to-day responsibilities as CIA director because he could have simply appointed a superlative manager as a second deputy director or strengthened the position of the executive director of the agency. The President could have run proposed candidates to head the various intelligence agencies by the DCI also without the new legislation.

In fact, President Bush had already taken several steps for the reorganization in some executive orders issued on August 27, 2004, in response to the 9/11 Commission's report and before the bills were introduced in Congress. One of these orders made the DCI "the principal adviser to the President for intelligence matters related to the national security," gave him the task to develop "objectives

[76] Ibid., pag. 56-57

and guidance for the Intelligence Community necessary, in the Director's judgment, to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source derived," and gave him directions to "establish common security and access standards for managing and handling intelligence," "establish, operate, and direct national centers of intelligence," "establish policies, procedures, and mechanisms that translate intelligence objectives and priorities approved by the President into specific guidance for the Intelligence Community," "develop, determine, and present with the advice of the heads of departments or agencies" an annual strengthened intelligence budget and the transfer of appropriated funds among agencies.[77] Moreover, the order gave the DCI veto power in appointing heads of intelligence organizations that are not Presidential appointees; directed him to decide standards and qualifications for intelligence personnel, and directed him to propose his own recommendations to Congress to support any Presidential nomination of the head of an intelligence service that is a Presidential appointee.

Even though one of the main proposals of the 9/11 Commission adopted by the Intelligence Reform Act was the creation of a National Counterterrorism Center, the second executive order issued on August 27, 2004, had already done it.[78]

[77] *Strengthened Management of the Intelligence Community*, Executive Order 13355, August 27, 2004, p. 1699
[78] *National Counterterrorism Center*, Executive Order 13354, August 27, 2004

The Shaping of the DNI's Authority

Issue	Senate bill	House Bill	Final Bill
Declassification of budget intelligence top line	Declassify budget top line	Retain classified budget top line	Retain classified budget top line
Budget execution	Intelligence funds do not flow through the Department of Defense to intelligence agencies	Intelligence funds flow through the Department of Defense	Intelligence funds flow through the Department of Defense
Chain-of-command protection	No chain-of-command protection	No need for chain-of-command provision	Specific provision requiring that implementation "respect and not abrogate" existing military chain-of-command statutes
Budget reprogramming	NID can reprogram unlimited amount of funds without approval of department/ agency heads	NID unilateral reprogram authority capped at 5% of department budgets	DNI unilateral reprogram authority capped at 5% of department budgets
Personnel transfers	DNI can transfer unlimited number of personnel without the approval of department/ agency heads	No unilateral personnel transfer authority	DNI's unilateral transfer authority is limited to 100 personnel for each new national intelligence center created
Personnel management	DNI can prescribe personnel policies and requirements for all personnel within the intelligence community, including military personnel	DNI personnel-policy authorities limited to civilian employees	DNI personnel-policy authorities limited to civilian employees
DNI control over military programs	Gives DNI primary control over all programs of the NSA, NRO, and NGA, including non-national (JMIP) military programs	Excludes from DNI primary control all military intelligence programs within the JMIP	Excludes from DNI primary control all military intelligence programs within the JMIP

Source: Gregory F. Treverton, 2009, p. 84

The President would not have needed to emit an executive order in a way of centralizing authority over the budget proposals of the intelligence's agencies to Congress. Such authority was already centralized in the Office of Management and Budget. The President might have emitted those orders in prevision of the Intelligence Reform Act and not because he thought such an improvement of the existing structure a good idea. He might also have hoped to forestall the act; so maybe the act should be viewed as a push to prevent his changes of mind of the executive orders. Only as long as there is a political consensus in behalf of greater centralization of intelligence will the Intelligence Reform Act be interpreted in the spirit of the 9/11 Commission's report, and with such consensus the President is likely to centralize without a legislative push. The President failed to forestall the Intelligence Reform Act, but the act might prove to have been a ruinous effort to forestall the President.

The Reform Act, finally enacted, combined the organizational provisions of the Senate bill with the additional domestic law enforcement in the House bill. The authority of the DNI was weakened by the main alterations to the organizational provisions in the Senate bill. The Director of National Intelligence "shall be appointed by the President, by and with the advice and consent of the Senate" and "shall have extensive national security expertise".[79] He is to serve "as head of the intelligence community", but he is to do so "subject to the authority, direction, and control of the President".[80] The DNI is to "oversee and direct the implementation of the National Intelligence Program."[81]

The DNI is to guide the formulation of budget requests by the agencies whose budgets are part of the National Intelligence Program and to formulate a strengthened budget to submit to the approval of the President. The DNI has a limited authority over the reallocations of appropriated funds among the agencies. The Reform Act limits the authority of the DNI over personnel.

[79] National Security Act of 1947, p. 12
[80] Ibid.
[81] Ibid.

The DNI is authorized to have a staff of 500 people who will come from the existing agencies. This transfer of personnel is expected to produce serious confusion in the intelligence community. Without a doubt it will include many lawyers, auditors, publicists, reviewers and so on, but in all likelihood it will be mainly composed of intelligence analysts.

As far as the new structure of the intelligence system is concerned, only two things emerge from this legislation. One is that the legislation, to a certain extent, subdues the centralizing push of the 9/11 Commission's report. The extent of centralization achieved by the act will emerge in the implementation process and will depend on President's decisions. Second, even though the legislation does not adopt the 9/11 Commission's recommendation to deprive the CIA of its paramilitary capability, it imagines the weakening of the agency. There will be a DNI with large powers and a large staff, and the National Counterterrorism Center will report to the DNI rather than to the CIA's Director. The National Intelligence Council, whose task is issuing the National Intelligence Estimates, will now report to the DNI and not to the DCI.

All the other components of national defense against terrorism that failed on 9/11 must be strengthened, even though many of them, especially the FBI, failed more than the CIA. The reason may be due to the fact that the CIA is a very unpopular agency in contrast to the FBI; in some places, spying and other clandestine operations are considered a dirty business. A more important reason is the psychological disproportion between failure and success in intelligence operations.

> *If the CIA fails to anticipate a surprise attack or some other surprising event, the failure is palpable; the attack, or the event, which as a result is averted, then the success, even if it is publicly disclosed, will fail to make a dramatic impact because nothing observable has happened.*[82]

The success was that nothing happened, and if nothing happens it is hard to imagine a disaster that is averted. That's the reason why the CIA's failures register

[82] Posner, 2005, p. 68

strongly in the mind of the public and are remembered and the successes forgotten, and the result is a negative image of the agency.

CHAPTER 3

AN IMPLEMENTATION OF THE 9/11 RECOMMENDATIONS

3.1 INTRODUCTION

Since the September 11, 2001 attacks, the United States have made an important progress in securing the nation from terrorism. After 9/11, the federal government tried to develop a security framework with the aim to protect the country from large-scale attacks. Such framework has led to considerable success in both preventing this kind of attack and limiting the operational ability of the Al-Qaeda group. However, as terrorism threats persist and continue to evolve, there is still a lot of work to be done. In addition to the threats that come from abroad, the nation must deal with the homegrown ones.

Over the past years, the Department of Homeland Security (DHS) has worked to strengthen and evolve the homeland security initiative.

> *Within the federal government, many departments and agencies contribute to the homeland security mission. The nation's armed forces are on the frontlines of homeland security by helping to significantly degrade Al-Qaeda capabilities to attack the United States and targets throughout the world. The Director of National Intelligence, the Central Intelligence Agency, and the entire Intelligence Community, of which DHS is a member, is producing more and better streams of intelligence than before. Multiple federal departments and agencies, including the Terrorist Screening Center (TSC) and the National Counterterrorism Center (NCTC) have made critical enhancements to the federal watch listing systems and to the coordination of the federal government's counterterrorism efforts.*[155]

The homeland security initiative goes far beyond the DHS and the federal government. It works directly with the law enforcement, state and local leaders,

[155] U.S Department of Homeland Security, *Implementing the 9/11 Commission Recommendations*, Progress Report 2011, p. 9

community-based organizations, and private sector partners to counter violent extremism at its source, using quite the same techniques and strategies that have been successful for decades in combating violent crime in American communities. The aim of this chapter is to analyze such initiatives and improvements taken starting from 9/11.

The public also has an important role in this new homeland security initiative. With the —If You See Something, Say Something— campaign, the DHS is increasing public awareness of indicators of terrorism, crime and other threats and also emphasizing the importance of reporting suspicious activity to the proper law enforcement authorities. Continuing efforts to better understand the risks confronting the homeland further strengthen the homeland security initiative.

3.2 CHRONOLOGY OF SEPTEMBER 11

September 11, 2001	Today
In early 1999, Osama Bin Laden convened operatives to Afghanistan to discuss the use of commercial aircraft as weapons and developed a list of potential targets in the United States.	Today this Administration has developed multilayered information sharing security strategy to target and identify both known and unknown individuals that may pose a threat to the United States wherever the operational planning might occur with the goal of preventing such people from entering the country.
In April of 1999, the hijackers began to obtain passports and visas for travelling to the United States.	DHS and other federal partners have built a capacity to more extensively vet those individuals applying for visas or travel to the U.S.
Between 1999 and 2001, many of the hijackers prepared for the 9/11 attacks while living in Germany.	The DHS, in collaboration with the Departments of Justice and State, has signed Preventing and Combating Serious Crime Agreements with 18 countries in order to share information about terrorists and criminals.
The hijackers began arriving in the U.S. in late April 2001 with tourist visas.	DHS partners with the Terrorist Screening Center, the National Counterterrorism Center and other federal entities to analyze travel-related data in order to better understand and anticipate the travel patterns of known or suspected terrorists.
Prior to 9/11, the hijackers enrolled in flight schools and conducted cross-country surveillance flights in order to identify aircraft that would produce their desired impact.	The Transportation Security Administration (TSA) has responsibility for ensuring that foreign students seeking training at flight schools do not pose a threat to aviation or national security.
During the spring and summer of 2001, several of the hijackers were apprehended by U.S. law enforcement for various traffic violations.	Today, 72 recognized fusion centers throughout the country serve as focal points at the state and local level for the receipt, analysis, gathering, and sharing of threat and vulnerability-related information. In addition, the Nationwide Suspicious Activity Reporting Initiative helps to train state and local law enforcement to recognize behaviors and indicators related to terrorism, crime and other threats while standardizing how those observations are analyzed and disseminated.

	Finally, state and local law enforcement officers can determine whether an individual is on a watch list through the National Crime Information Center.
On the morning of 9/11, hijackers passed through security checkpoints at four U.S. airports, allegedly carrying knives, box cutters and concealed weapons on their person or in carry-on luggage.	Multilayered security measures are now in place to enhance aviation security including the prescreening of passengers; the deployment of new technologies; and training of airport security and law enforcement personnel to better detect behaviors associated with terrorism.
Although eight of the hijackers were randomly selected for additional screening and a gate agent flagged two as suspicious, none were prevented from boarding their flights on 9/11.	Today, TSA's Behavior Detection Officers utilize non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers who exhibit behaviors that indicate they may be a threat to aviation and/or transportation security and refer them for additional screening. TSA also conducts screening of passengers at boarding gates based on current intelligence and passengers of interest.
At 8:19 AM, flight attendants and passengers began reporting hijackings of the aircraft via air phone.	Following 9/11, all commercial aircraft have been secured through the hardening of cockpit doors.
Throughout the morning of September 11, 2011, air traffic control operators, military personnel and first responders on the ground lacked situational awareness of what other agencies were doing to address the developing crisis.	Through the use of mobile and fixed site technologies, voice radio systems used by first responders are more interoperable than ever before.

Source: U.S Department of Homeland Security, *Implementing the 9/11 Commission Recommendations*, Progress Report 2011, pp. 7-8

3.3 THE EXPANSION OF INFORMATION SHARING

RECOMMENDATION: "Provide Incentives for Information Sharing"[156]

During the last years, the DHS strengthened and improved the homeland security initiative for a better reduction and defense against threats. Such concept is based on the idea that the hometown security gives life to the homeland security. The DHS role is to ensure resources and information availability to state and local law enforcement through close partnerships with federal, state and local governments, community-based organizations, and private sector partners. In this way it gives to those on the frontlines the tools to protect local communities. Thanks to this method, a number of critical characteristics and information sharing that did not exist before 9/11 are now included. The DHS puts together information and shares it across the country in the best way that protects the homeland.

- **National Terrorism Advisory System**

In April 2011, the implementation of the new National Terrorism Advisory System (NTAS) was announced by the DHS that replaced the previous already obsolete color-coded alert system. The NTAS allows a more effectively communication of information about terrorist threats by providing to the public timely, detailed information and recommended security measures. Under the NTAS, the DHS coordinating with other federal entities gives detailed alerts to the public when the federal government receives information about a specific, credible terrorist threat to the United States. The NTAS alerts give a brief summary of the possible threat.

- **Information Sharing**

Since 9/11, the federal government has tried to improve the connection between collection and analysis on transnational organizations and threats. The

[156] The 9/11 Commission Report, 2004, p. 417

DHS with the help of the FBI has re-concentrated its information sharing and production labors in order to better face the needs of state, local governments and private sector partners. Moreover, the DHS and the FBI provide training programs for local law enforcement in order to help them with the identification of indicators of terrorist activity. The DHS continues to "improve and expand the information-sharing mechanisms by which officers are made aware of the threat picture, vulnerabilities, and what it means for their local communities."[157]

- **Countering Violent Extremism**

The efforts of the Department to work with state and local officials and also with community groups are concentrated on Countering Violent Extremism (CVE). During the past year the DHS developed a training curriculum for state and local law enforcement with a focus on community-oriented policing that may help frontline personnel to identify activities that indicate possible terrorist activity and violence.

- **Fusion Centers**

The role of the DHS is also to support the state and the main urban area fusion centers. The DHS "has deployed Homeland Secure Data Network systems to fusion centers"[158], in order to enable the federal government share of information and intelligence with state, local, tribal, territorial, and private sector partners. It has also collocated federal intelligence officers at fusion centers which role is to act as the primary intermediary between the federal governments and its partners.

- **Federal Partners**

The DHS does not work alone. He has some partner with who it works for some information sharing initiatives, it supports law enforcement operations and protects the country from terrorists and other threats.

[157] Implementing the 9/11 Commission Recommendations, 2011, p. 12
[158] Ibid. p. 12

- **Tribal Partners**

Thanks to the Obama Administration there has been an effort to create a strong relationships with Tribal governments and law enforcement across the nation.

- **Private Sector Partners**

The DHS facilitated a more effective and rapid communication with key organizations trying to improve the coordination of private sector engagement across the Department.

- **International Engagement**

Also the information sharing has been expanded among international partners. The DHS has signed the Preventing and Combating Serious Crime (PCSC) Agreements with 17 Visa Waiver Program (VWP) countries and one non-VWP country with the aim of sharing information about terrorists and criminals. It has also signed 12 international agreements for the promotion of collaboration in science and technology.

- **Nationwide Suspicious Activity Reporting Initiative**

The DHS has worked with its numerous partners in order to expand the Nationwide Suspicious Activity Reporting Initiative (NSI). Such initiative is an

> *administration effort to train state and local law enforcement to recognize behaviors and indicators related to terrorism, crime and other threats; standardize how those observations are documented and analyzed; and enhance the sharing of those reports with law enforcement and communities throughout the country.*[159]

- **"If You See Something, Say Something" Campaign**

The public also gives its help to the homeland security through the expansion of the "If You See Something, Say Something" campaign. It is a simple and but very effective initiative that collect public awareness of indicators of terrorism and crime,

[159] Ibid., p. 14

and underlines how it is important to report suspicious activity to law enforcement authorities.

3.4 THE DEVELOPMENT AND IMPLEMENTATION OF RISK-BASED TRANSPORTATION SECURITY STRATEGIES

RECOMMENDATION: "Develop a Risk-Based Plan for Transportation Security"[160]

The DHS focuses on "risk-based, intelligence-driven security"[161] across all means of transport. Security assessments across aviation, maritime, and surface transportation sectors are the result of significant advances in risk-based security. In 2010, the Transportation Security Administration (TSA) gave to Congress the Transportation Sector Security Risk Assessment report. Such report aim is to examine the potential threats, vulnerabilities, and consequences of a terrorist attack that involve the transportation system of the nation.

◦ Aviation Security

After the terrorist attack that was attempted against the Northwest Airlines Flight 253 on December 25, 2009[162], the DHS worked with the International Civil Aviation Organization (ICAO) on an initiative that would have strengthened global aviation against terrorists' threats. The Declaration on Aviation Security was then adopted by nearly 190 countries. Such Declaration created a historic new foundation for aviation security that better protected the entire global aviation system and made air travel safer and more secure.

◦ Surface Transportation Security

The surface transportation sector has a completely different operational environment. The DHS task is to help secure surface transportation infrastructure through "risk-based security assessments, critical infrastructure hardening, and close partnerships with state and local law enforcement partners."[163]

---

[160] The 9/11 Commission Report, 2004, p. 391
[161] Implementing the 9/11 Commission Recommendations, 2011, p. 16
[162] See *Attempted Terrorist Attack on Northwest Airlines Flight 253*, Report of the Select Committee on Intelligence United States Senate, 2010
[163] Ibid., p. 18

- **Maritime Transportation Security**

The DHS aim is to strengthen maritime transportation security with the help of a risk and technology based approach that evaluates vulnerabilities and mitigates threats across all potential ways. With this purpose, the U.S. Coast Guard (USCG) has published a series of regulations that will increase the security of U.S. ports, ships, and facilities.

3.5 STRENGHTENING AIRLINE PASSANGER PRE-SCREENING AND TARGETING TERRORIST TRAVEL

RECOMMENDATIONS: "Improve airline passenger pre-screening"[164] and "target terrorist travel"[165]

Before 9/11, the screening of passengers arriving to the United States was just the DOS visa process and the inspection of a person by an immigration officer at the entry port. During the last ten years, the DHS has improved its ability to detect threats. It has implemented pre-departure programs for U.S. flights and improved security measures in order to reinforce the safety and security of all passengers, using real-time, threat-based intelligence and multiple levels of security.

- **Identification Pre-Departure**

The DHS, the intelligence and law enforcement communities have developed new mechanisms that are able to identify high-risk travelers before the departure. The U.S. terrorist watch list criteria and nomination processes have been reformed, the capabilities regarding information sharing have been improved. Such improvements will help to prevent the entry of dangerous individuals to the United States.

- **Improved Analysis of Travel-Related Data**

Today there are four centers across the federal government that give information about potential terrorist travel: the National Counterterrorism Center (NCTC), the Terrorist Screening Center (TSC), the National Targeting Center, and the Human Smuggling and Trafficking Center.

[164] The 9/11 Commission Report, 2004, p. 393
[165] Ibid., p. 385

- **Visa Waiver Program**

With the Visa Waiver Program VWP, the nationals of 36 participating countries are not allowed to travel to the United States for stays of 90 days or less without a visa.

- **Visa Security**

With the Visa Security Program (VSP), the U.S. Immigration and Customs Enforcement (ICE) uses trained special agents overseas to high-risk visa activity posts which aim is to identify potential terrorist and criminal threats before can they reach the United States. The DHS, with the help of federal partners has worked to "improve and expand procedures for vetting immigrant and nonimmigrant visa applicants, asylum applicants, and refugees."[166]

- **Passenger Name Records and Advance Passenger Information**

One of the most important thing is the DHS' improved ability to use information in order to target and identify both known and unknown individuals that are a threat to aviation and to the United States, and to prevent them from flying to or entering the United States.

- **Secure Flight**

The DHS improved Secure Flight prescreening the totality of passengers on flights flying to, from, or within the U.S.. In order to facilitate a secure travel for all passengers, this program helps also to prevent the misidentification of passengers that have names similar to individuals on government watch lists.

- **Program Pre-Departure**

The U.S. Customs and Border Protection (CBP) has reinforced its in-bound targeting operations in order to identify high-risk travelers that are not admissible into the U.S..

[166] Ibid., p. 24

- **Pre-clearance Agreements**

The pre-clearance agreements allow the DHS to screen travelers and their baggage before the takeoff.

- **Immigration Advisory Program**

The Immigration Advisory Program enables the use of advanced targeting and passenger analysis information by the CBP officers that are posted at foreign airports with the aim to identify high-risk travelers at foreign airports before they board U.S. flights.

- **Trusted Traveler Programs and Enhancing of the Traveling Experience**

The CBP has increased the registrations in its traveler programs in order to facilitate legitimate travel and effectively use screening and security resources.

- **Risk-Based Screening Strategy for the Future**

The Administration still focuses its attention on the implementation of risk-based measures that will strengthen aviation security and improve the experience of passengers.

3.6 THE IMPROVEMENT OF SCREENING FOR EXPLOSIVES

RECOMMENDATION: "Improve aviation security through enhanced explosive screening"[167]

Thanks to annual appropriations and the Recovery Act, the TSA has implemented the use of new technologies that will detect the next generation of threats. Before 9/11 there were limited federal security requirements for cargo and baggage screening, while today all baggage is screened.

- **Enhancing Screening Technologies**

The Advanced Imaging Technology (AIT) is used to screen passengers for metallic and nonmetallic threats. The Explosives Trace Detection (ETD) units instead, are used to screen articles that are carried on, baggage already checked, and passengers for explosive residue. The Advanced Technology X-Ray machine is used to scan carry-on baggage and to provide a clear image to the operator. Bottled Liquid Scanners are devices able to detect flammable liquids and explosives.

- **Canines**

Canine teams are used by the TSA to screen air cargo at the nation's highest cargo volume airports. They are able to detect explosives in all sectors: aviation, maritime transportation and mass transit.

- **Cargo Security**

Before 9/11 there were no federal security requirements for cargo screening. But now all cargo that leaves U.S. airports is screened as passenger baggage. Moreover, in 2011 a series of new initiatives that made the system stronger, smarter and more resilient were outlined.

[167] The 9/11 Commission Report, 2004, p. 393

3.7 THE REINFORCEMENT OF EFFORTS IN ORDER TO DETECT AND REPORT BIOLOGICAL, RADIOLOGICAL AND NUCLEAR THREATS

RECOMMENDATION: "Strengthen counter proliferation efforts to prevent radiological/nuclear terrorism"[168]

A coordinated government approach is the most important requirement to counter nuclear, biological and radiological threats. The Domestic Nuclear Detection Office (DNDO), in collaboration with agencies across federal, state and local government, works to prevent and deter attacks with the use of nuclear and radiological weapons. The Office of Health Affairs (OHA) does not only coordinate the Department's biological and chemical defense activities but provides also medical and scientific expertise that support preparedness and response efforts.

- **Nuclear Detection**

The DNDO task is to improve the capability of the nation for detecting and reporting attempts that are not authorized to import, develop, or transport nuclear or radiological material that could be used against the United States.

- **Nuclear Forensics**

Another responsibility of the DHS is to advance the nation's nuclear forensics capability. Law enforcement, intelligence information and nuclear forensics support the identification of individuals involved in attacks that use radiological or nuclear weapons.

- **Counter-Proliferation**

One of DHS's main priorities is to prevent the illegal obtainment of U.S. military products and sensitive technology by terrorist groups and hostile nations. The Counter-Proliferation Investigations program's role is to supervise investigative activities connected to such violations.

[168] The 9/11 Commission Report, 2004, p. 381

- **Nuclear/Radiological Immediacy and Response**

The FEMA's task is to give detailed information with regard to roles, responsibilities, and instructions for radiological and nuclear threats to planners of all levels of government, the private sector, and non-governmental organizations. The aim of the Radiological Emergency Preparedness Program is to focus on "planning and preparedness for threats that could affect the nation's commercial nuclear power plants."[169]

- **Protection Against Biological Threats**

A great progress has been made by the DHS to prepare the nation, the federal, the state, and local governments to respond to biological attacks.

[169] Ibid., p. 33

3.8 THE PROTECTION OF CYBER NETWORKS AND OF CRITICAL PHYSICAL INFRASTRUCTURE

RECOMMENDATION: "Assess critical infrastructure and readiness"[170]

After September 11, significant moves were made by the DHS in order to improve the security of the critical physical infrastructure of the nation and also its cyber infrastructure and networks. New important tools were created, such as the National Cyber security Protection System (NCPS) and the National Cyber security and Communications Integration Center (NCCIC). The DHS developed the National Infrastructure Protection Plan (NIPP), a risk management framework useful at all levels of government, private industry and nongovernmental entities.

- **Safeguard of the Cyber Infrastructure and of Networks**

The current threats to cyber security require the involvement of the whole society in order to block wicked actors and improve capabilities of defense. The DHS responsibility is to protect "the federal executive branch civilian agencies and to guide the protection of the nation's critical infrastructure and connections to cyberspace."[171]

- **Protection of Infrastructure**

Since 2006, the DHS has provided funds to programs that allowed the protection of critical infrastructure from terrorism. Such programs granted "support security plans, facility security upgrades, training, exercises, law enforcement anti-terrorism operations, and capital projects for risk mitigation of high threat infrastructure."[172]

[170] The 9/11 Commission Report, 2004, p. 428
[171] Implementing the 9/11 Commission Recommendations, 2011, p. 35
[172] Ibid. p. 38

RECOMMENDATION: "Allocate homeland security funds based on risk"[173]

Since its creation, the DHS has awarded "more than $31 billion based on risk to build and sustain targeted capabilities and strengthen state and local prevention efforts across the homeland security enterprise."[174]Moreover, it has given priority to grant-funded prevention activities that support local homeland security efforts in order to address homegrown extremism.

RECOMMENDATION: "Track and disrupt terrorist financing"[175]

Since 9/11, the DHS has expanded in a significant way its ability to track and disrupt terrorist financing. Such tool is one among many that the U.S. Government uses for countering terrorism.

An important initiative was played by the ICE in combating bulk cash smuggling, a strategy that criminals use for trying to move illicit proceeds across transnational borders. The ICE established also the National Bulk Cash Smuggling Center, a "24/7 operations and intelligence facility which supports federal, state, local, and foreign law enforcement efforts to identify, investigate, and disrupt bulk cash smuggling activities throughout the world."[176]

RECOMMENDATION: "Improve interoperable communications at all levels of government"[177]

After the attacks, the DHS has improved its strategies in order to transform and reinforce interoperable communications across the country.

[173] The 9/11 Commission Report, 2004, p. 396
[174] Implementing the 9/11 Commission Recommendations, 2011, p. 42
[175] The 9/11 Commission Report, 2004, p. 382
[176] Implementing the 9/11 Commission Recommendations, 2011, p. 43
[177] The 9/11 Commission Report, 2004, p. 397

- **Enhancing Interoperability through the Office of Emergency Communications**

Federal, state, and local governments face many challenges to address interoperability in their wireless communications. It is complicated to establish national interoperability performance goals and standards, and to balance them with the flexibility that is required to deal with differences in state, regional, and local needs and conditions. As no single group can address interoperability challenges alone, the "partnership, leadership, and coordinated planning of everyone involved is required."[178]

RECOMMENDATION: "Establish a unified incident command system"[179]

After 9/11, the DHS has taken great steps in the establishment and improvement of a unified incident command system that responds to many different threats that range from natural disasters to coordinated attacks.

RECOMMENDATION: "Prioritize private sector preparedness"[180]

Since the attacks, the DHS has given priority to private sector preparedness through many different programs. Some of the most important are the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep™) - a partnership between DHS and the private sector with the aim to enable private entities to receive emergency preparedness certification-, and the Ready Business campaign –an initiative that provides materials to businesses of all sizes and encourages business continuity planning and crisis management-. The private sector was also given priority through the development and deployment of new technologies, and the incorporation of private sector partners.

[178] Implementing the 9/11 Commission Recommendations, 2011, p. 44
[179] The 9/11 Commission Report, 2004, p. 397
[180] Ibid., p. 398

3.9 THE SUPPORT OF THE SECURITY OF U.S. BORDERS AND IDENTIFICATION DOCUMENTS

RECOMMENDATION: "Standardize secure identification"[181]

Important steps have been made to reinforce security, reduce fraud and improve the reliability of personal identification documents. The DHS improved also privacy safeguards and changed the way in which travelers enter the United States within the Western Hemisphere by implementing the Western Hemisphere Travel Initiative (WHTI) and from other countries around the world by the "Visa Waiver Program, Visa Security Program and US-VISIT biometric identity and verification process.[182]

RECOMMENDATION: "Integrate border security into larger network of screening points that includes the transportation system and access to vital facilities"[183]

The protection of the borders of the nation has great importance for homeland security, as well as it has the economic prosperity. During the past years, the DHS has used personnel, technology, and resources to the Southwest border as never before. Security improvements have been made also along the Northern border, with investments in additional Border Patrol agents, technology, and infrastructure. Another great improvement was the effort to increase the security of the nation's maritime borders.

[181] Ibid., p. 390
[182] See Implementing the 9/11 Commission Recommendations, 2011, p. 51 - 56
[183] The 9/11 Commission Report, 2004, p. 387

3.10 THE CONTROL OF ROBUST PRIVACY AND CIVIL RIGHTS AND CIVIL LIBERTIES SAFEGUARDS

RECOMMENDATIONS: "Maintain Civil Liberties While Protecting Security"[184] and "Safeguard Individual Privacy When Sharing Information"[185]

From the beginning of the policymaking process, the DHS involves its Privacy Office and Office for Civil Rights and Civil Liberties (CRCL), "building in privacy and civil rights and civil liberties protections into all of its operations, policies and technology deployments."[186]

The Privacy Office of the DHS is the first privacy office required among any federal agency. The CRCL task is to support the mission of the Department in order to secure the nation, and at the same time, to preserve individual liberty, fairness, and equality under the law. The two offices together provide the DHS intelligence professionals a training on privacy, civil rights and civil liberties.

[184] Ibid., p. 394-395
[185] Ibid., p. 394
[186] See Implementing the 9/11 Commission Recommendations, 2011, p. 63

3.11 THE INTELLIGECE REFORM DEBATE

The intelligence reform debate has a non-definitive aspect that reflects both the difficulties of the issues and choices involved and the boundless enthusiasm of reform advocates. Even though there are no doubts that improvements can be made in intelligence, determining how efficient an inefficient and intellectual process may be is still ambiguous. There is a big difference between government-based reviews of the intelligence community, which tend to accept the status quo and so suggest small changes. The executive branch has rarely demonstrated enthusiasm for major reforms.

Such statement is explained by three factors. First, many policy makers believe that their most important needs are usually met. Second, many reforms' proposals would require a greater involvement of policy makers that they prefer to avoid. Third, many policy makers understand the fragilities of the intelligence community and fear the possibility that things could be made worse..

The truth is that, despite the numerous attempts to reform intelligence, revolutionary proposals tend to be ignored or, at best, to be severely moderated before being enacted. What is certain is that the debate over intelligence reform will go on with more attention during crises or after incidents deemed to be intelligence failures.

CHAPTER 4

CONCLUSIONS

4.1 INTRODUCTION

Thirteen years after the September 11 attacks, the work of the Department of Homeland Security is still going on but many challenges remain. However, the United States are now stronger than before.

Over the past ten years, a great stride has been made to secure the nation against a large attack or disaster, to protect critical infrastructure and cyber networks, and to engage a broader range of Americans in the shared responsibility for security. The United States are also a more prepared now, and are able to rebuild even stronger after a major crisis or disaster.

The goal of the reorganization instituted by the Intelligence Reform Act was and is to prevent another surprise attack to the United States. Yet, the history demonstrates that there have been many different surprise attacks that could have been anticipated, but it is not easy even for intelligence specialists to connect the dots. Failures will remain despite the attempts at reforming and improving intelligence. The future of intelligence is a doubtful one, and we don't know if the United States will be able to prevent a future attack with the dimensions of the 9/11 ones.

4.2 THE MAIN SUCCESSFUL SURPRISE ATTACKS

The central part of my work described how the 9/11 Commission faced the issue of the optimal organization of the U.S. intelligence system, and how Congress followed that approach with the production of a sense of uncertainty about how the system would have changed. Analyzing the history of surprise attacks may be useful to find alternative organizational approaches, because, as we know, it was the fear of attacks that moved the idea of reorganization. All surprise attacks follow a model, and the 9/11 attacks followed a model too. Once the model is clear, the question of whether a reorganization of the intelligence system is a sensible response to the threat of similar attacks will become a debating point.

Before September 11 the biggest surprise attack had been the Japanese attack on Pearl Harbor in 1941. Roberta Wohlstetter[115], with her book Pearl Harbor: Warning and Decision, tries to explain the causes of the U.S. intelligence failures that led to the 1941 surprise attack. In the years before the attack, U.S. code breakers were reading with a certain regularity much of the Japanese military and diplomatic traffic. However, the Japanese attack came as both a tactical and strategic surprise. On the strategic level, because U.S. intelligence analysts considered unlikely the idea of an attack as Japan could not expect to win a hypothetical subsequent war. On several occasions during 1940-41 even tough U.S. forces were put on high alert no attack came. At the end, they convinced themselves hat the logical place for a Japanese attack would be in the Philippines. On the tactical level, instead, the attack came as a surprise because warning mechanisms were not deployed. When a satisfactory response to a threat is hard to conceive the tendency is the denying of the threat. Even though some signals indicated Pearl Harbor as possible objective, more other signals indicated different possible objectives.

[115] See Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*, Stanford University Press, Stanford, CA, 1962

At the beginning of 1968, during the Tet[116] holiday period, an offensive of the Viet Cong and North Vietnamese forces against South Vietnam's cities shocked the U.S.. Exactly as in the Pearl Harbor attack, numerous were the signals of the impending offensive, but none of them was taken into account. Indeed, some Viet Cong attacked several South Vietnamese cities the day before the beginning of the Tet holidays. Such attack should have been considered as a confirmation of predictions of cities offensive during Tet.[117] It seemed so unreal that the enemy would have tried to take over South Vietnam's cities that wasn't even considered..

A third example of a successful surprise attack before 9/11 was the one made by Egypt and Syria to Israel in 1973, on the Jewish holiday of Yom Kippur. After launching a surprise air attack that opened the Six-Day War in 1967, Israel was aware that the Arab states would have reciprocated. As it is typical for surprise attacks, the warnings of an impending attack were abundant, but nothing was done. Both in the Pearl Harbor and Yom Kippur case the victim thought that its enemy would have needed more time to gain enough strength for a successful attack, but they were wrong.

[116] The festival which best epitomizes Vietnam's cultural identity is Vietnamese New Year or Tet, which is the phonetic deformation of "Tiet", a Sino Vietnamese term which means "Joint of a bamboo stern" and in a wider sense, the "beginning of a period of the year".
[117] Spencer C. Tucker, Vietnam, University Press of Kentucky, 1999

Even though common features may be found on the reported examples, they are too little to demonstrate that they always affect successful surprise attacks.

Some of the common features were:

- The weakness of the attacker to have much hope of prevailing;
- The victim's perception contributed to the enemy's weakness in the failure to anticipate the attack;
- The victims lacked in understanding the attacker's intentions and capabilities;
- The victim's thought that the main danger would take place elsewhere or in the future;
- The victims interpreted warning signs as fitting a preconceived conception of the intentions and capabilities of the enemy;
- The false alarms or deliberated deception to the victim;
- The victim's state of denial with regard to forms of attack that would be hardest to defend against;
- Intelligence officers were reluctant for career reasons to challenge the opinion of their superiors;
- Clarity and credibility lack of the warnings to local commanders of impending attacks.

The benefits of avoiding a disaster must be discounted or multiplied by the probability that the disaster will occur if there are no additional measures. What emerges is that

> the lower the perceived probability of attack, and the less harm the attack will do if it occurs, and the higher the costs of preventive measures, including the costs created by false alarms, the less likely the measures are to be taken.[118]

Through an analysis of the events, what emerges is that surprise attacks cannot be prevented in a reliable way. As some attacks can be prevented while others not, for those that occur the best that can be done is to mitigate the worst

[118] Posner, 2005, p. 87

possible consequences. The question that raises spontaneously is: Which is, then, the solution for avoiding or preventing surprise attacks?

The only thing that could be done at this point is to consider a possible organizational solution to the problems of intelligence described throughout the work.

4.3 IS A REORGANIZATION OF THE U.S. INTELLIGENCE THE SOLUTION?

After examining the successful surprise attacks and their difficulties that explain their success, it's time to consider if some of these difficulties may be overtaken through a reorganization of the intelligence system, a bigger focus on the 9/11 Commission's recommendations and their legislative implementation. As noted throughout the chapters, the failure to anticipate the 9/11 attacks does not seem to be dued to the U.S. intelligence organization system.

> *Efforts at comprehensive administrative reorganization, like other governmental programs, are symbols of the possibility of meaningful action. Confessions of impotence are not acceptable; leaders are expected to act, and reorganizations provide an opportunity to symbolize action. Presidents who promise reforms apparently do not suffer if they fail to implement them. Announcing a major reorganization symbolizes the possibility of effective leadership, and the belief in that possibility may be of greater significance than the execution of it.*[119]

The reorganization solution may be a questionable response to a problem that is not supposed to be a problem of organization. Even if it may not be costly in financial terms, it imposes substantial no pecuniary costs.

Reorganization may solve a problem that was not an organizational one. It may "wake up" the accustomed ways of how things are done in an organization and this because "people in organizations are talented at normalizing deviant events, at reconciling outliers to a central tendency, at producing plausible displays, at making do with scraps of information, at translating equivocality into feasible alternatives,

[119] James G. March and Johan P. Olson, *Organizing Political Life: What Administrative Reorganization Tells Us about Government*, 1983, American Political Science Review, 77, pp. 281-296.

and at treating as sufficient whatever information is at hand."[120] But if on one side reorganization may facilitate needed personnel changes, on the other, the costs of transition must be considered. The aim of an organization is the coordination of activities. It seems natural to think that an organization is an efficient method, but this idea is not completely true because knowledge requires a costly transfer. Because of the cost, the "boss" of a complex system will not have all the information he needs in order to be able to exercise control in an intelligent way.; from here the importance of decentralized coordination methods. After realizing the importance of decentralization another important step is to make the autonomous divisions separate agencies.

As we have seen, the 9/11 Commission's mainly accuse regarding the failure to anticipate the 9/11 attacks was on inadequate sharing of intelligence among the different intelligence agencies. It thought that a more centralized intelligence structure would have been an indispensable part of the cure. The problem of information sharing is as diffused within agencies like the CIA and the FBI as among agencies.

The aim of intelligence is learning about the capabilities and intentions of potential enemies. Intelligence data are collected by spies and through the analysis of publicly available materials. The data are then given to analysts who piece them together and their results are finally forwarded to the office responsible for policy.

A criticism to the U.S. intelligence during the collection phase is that its spies are not always sufficiently used; this is due to the fact that spying is a dangerous occupation. Most spies are nationals of the country spied, and so traitors. Covert operations usually intended to the achievement or the exploitation of intelligence, seems to be counter-productive.

> Except in time of war, moreover, running spies in foreign countries is a hostile as well as an illegal act directed against a friendly nation, and so when a spy is caught the country he is spying for is likely to suffer a diplomatic setback.[121]

[120] Richard L. Daft and Karl E. Weick, Toward a Model of Organizations as Interpretation Systems, Academy of Management. The Academy of Management Review, 1984, pp. 284 -294
[121] Ibid. p. 101

Technical means of spying such as satellites are considered "cleaner", and that's the reason why the U.S. prefers investing in technical rather than in human espionage.

Open-source materials are very important for intelligence. Journal and other producers of public information are sometimes more specialized and have a greater access to target groups than intelligence professionals. One reason could be that the intentions of a political enemy are so difficult to be recognized that an intelligence agency might not have advantages over outsiders in guessing at such intentions. The limitations of resources available for defense and the possibility of thinking about indefinite threats will force intelligence officers to overlook less probable events. The reluctance of intelligence officers in sharing information with each other is due to their fear of penetration and leaks. Such reluctance makes it difficult to assemble all information. Even when intelligence services share information there is reluctance in the identification of information sources. Moreover, intelligence officers are reluctant in sharing information with the officials, the ones in charge of deciding which action, if any, must be taken. Such reluctance is understandable because people outside the intelligence community are more likely to let out information than intelligence officers are.

The lulling effect of false alarms "builds conservatism into warning intelligence."[122]The best thing should be an intelligence service able to anticipate "most" surprise attacks with the "fewest" false alarms.

Intelligence officers should avoid definite predictions, because as it is known, the more precise a prediction is the more it can be wrong. Their reluctance in sounding the alarm is due to their tendency to call for more information before acting. As Cynthia M. Grabo explains:

> *It is usually safer to fail to predict something which does happen than to make a positive prediction that something will happen and it does not. In the first case, it can always be maintained that there was insufficient evidence to come to a positive judgment.* [123]

[122] Ibid., p. 104
[123] Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 2002, p. 168-169

The best thing to do is acquire the more possible information in order to make a correct prediction.

Sometimes it happens that intelligence officers hesitate to update predictions on the basis of new information. Such hesitation demonstrates that the change of a prediction on the basis of new information is seen as an acknowledgment that the previous prediction was not correct. They should weasel out of making predictions in contrast with their colleagues and superiors' predictions.

As surprise attacks are low-probability events, they tend to occur at long intervals. When an attack occurs, however, everyone is hyper-alert and the tendency of not to warn is suspended and reversed. Every month that passes without an attack on the U.S. the alertness of the intelligence services becomes more and more weak. The growing interval brings to hope that the greater danger has gone. If alertness remains high, moreover, it might distract the intelligence system from threats even greater than the precedent one that caused the state of alert. Eventually, the problem could be overcame by simply expanding the system so that it could attend to the other threats without the reduction of the resources allocated to what is expected to be the greatest threat.

The problem of delayed response is also serious, due to the difficulty of getting people worried about future threats. When the Cold War ended and a Democratic President not much interested in national security affairs was elected, the problematic side of the CIA also known as the clandestine service was cut back. The 9/11 attacks, beside the Weapons of Mass Destruction (WMD) fiasco, indicated that the cutback had gone too far; but it is not easy to produce intelligence officers with the required proficiency.

While intelligence analysts have a propensity for making vague and optimistic predictions their reluctance to share with other information on which they are planning to base their predictions impede effective analysis. This tendency has not to be mixed up with the service's concern for the prevention of leakage and penetration.

A greater danger of leaks is found when the intelligence service, having completed its analysis, forwards the results to the action-level officials.

Other obstacles are introduced in the interaction between intelligence officers and officials.

At the policymaking level, officials tend to be their own intelligence officers. Such tendency is reinforced by

> *a national distrust of intelligence professionals that is based on the known reluctance of civil servants to share information with their superiors. The civil servant's reluctance to be candid with its superiors is rational. The better informed the superior is, the easier it is for him to challenge the advice he receives from his subordinates. Realizing this, they will be chary about conveying information to their superior, who, aware of this tendency, will tend to discount the advice he receives from his subordinates and to turn elsewhere for guidance.*[124]

The career tensions between intelligence professionals and their political superiors are made worse by politics.

Cognitive limitations reinforce the careerist impediments to reliable intelligence analysis. The most important one is the inability of the mind to process all the data presented to it by the senses. Due to the volume of data, what is considered usable is a product of pre-selection. The information collected and forwarded to the intelligence analyst will be so selected, shaped and interpreted.

Another cognitive limitation derives from the difficulty that people have in taking in a serious way dangers that have never materialized before. They are more likely to think about uncertain events in terms of frequency rather than probability. It seems that something that has happened more than once in the past may occur about as often in the future, while a probability of something that has never happened but might yet, tend not to be taken seriously. The result is that what has happened has a greater influence on planning for the future than what might happen.

The 9/11 Commission's report is an example of such limitation, because it is mainly concerned with how to prevent a similar repetition of the 9/11 attacks and neglects possibilities that have not yet materialized. Such tendency is an obstacle to the maintenance of a political commitment to adequate support of intelligence

[124] Posner, 2005, p. 115

services because the probability of a future attack tends not to impress people as a real danger.

The failure to prevent the 9/11 attacks was due to the fact that the imaginable covers a too broad surface, a reason for focusing on things that have never happened before.

The last cognitive tendency is the attribution to the leaders of a foreign nation or group of the same basic knowledge, psychology, values and reasoning processes as one's own. Such behavior has to be considered natural because it would be extremely difficult to coordinate our behaviors with the other ones'.

To conclude, what emerges is that a more effective prevention of surprise attacks rather than a reorganization of the intelligence system, might be a policy of preventive war designed to preempt surprise attacks.

4.4 CRITICS TO THE COMMISSION'S RECOMMENDATIONS

The Commission's recommendations that created the DNI and the National Counterterrorism Center have been at the center of a wave of criticism.

Some critics argued that the Commission had been reductionist in its focus on the intelligence reform. Even if the DCI have had sufficient authority and have had reorganized and transformed the intelligence community, the 9/11 attacks probably would not have been prevented because the intelligence community can never guarantee with certainty a success in stopping a terrorist. Moreover, even if the intelligence community would have predicted the use of aircraft as weapons, policy makers might have not been able to increase airline safety because of the resulting cost to airlines and passengers. The fact that many governmental failures, unrelated to the intelligence community, occurred before 9/11 does not mean that the intelligence community itself did not fail. The weakness of governments in other areas means that there is a need to improve counterterrorism activities.

> *Intelligence reform is needed not only because intelligence is one link in the chain of executive branch counterterrorism activities, but also because it is critical for improving the performance of each executive branch activity against terrorism.*[125]

It is unconceivable to expect the intelligence community to stop all terrorist attacks. However, the fact that the intelligence community will never perform in a perfect way does not justify the existence of problems in the intelligence community.

Other critics argued that only if people would have been better could the intelligence community's problems have been solved. Good people are the most important prerequisite for the success of an organization. However, even the best personnel cannot make an organizational structure work in a satisfactory way.

Another wave of critics argued that removing the DNI's responsibility for running the CIA would have deprived the DNI of "troops". But such criticism missed

[125] Peter Berkowitz, *The Future of American Intelligence,* Hoover Press, 2005, p. 92

the point of the Commission's recommendation, because the Commission's recommendation was designed to give the DNI authority for managing the intelligence community and controlling funds and setting standards for security, information technology, and personnel.

Other critics argued that a strong DNI would reduce the conduct of "competitive analysis" and decrease the quality of intelligence provided to policy makers. "Competitive analysis refers to the formal process by which the major intelligence agencies with all-source analysis capabilities work together to produce national intelligence estimates (NIEs)."[126] The creation of a DNI would not harm competitive analysis but would instead improve it. The DNI's integration of the intelligence community would both aid the military's actual operations and provide policy makers with better strategic information to guide the overall deployment of military forces.

Different critics were worried about the fact that the Commission did not take into account major changes in the intelligence community since 9/11. In fact, the fundamental institutional weakness of the DCI in statute and in practice was not remedied after 9/11.

The last wave of critics underlined the fact that a structural reform would not solve all the problems of the intelligence community.
However, structural reform as said before, affects the incentives guiding personnel.

> *The legislation creates a performance-based system: The DNI is given sufficient authorities to manage the intelligence community, with flexibility in how to employ those authorities and structure the national intelligence centers and other community entities.*[127]

What is really important is that the Intelligence Community, for a variety of reasons, failed to bring together a range of information that could have greatly improved its chances of preventing the Usama Bin Laden plan to attack the United States on September 11, 2001.

[126] Ibid., p. 96
[127] Ibid., p. 100

As a consequence, the Community missed the opportunity to disrupt the September 11 plot; to try to unravel the plot through surveillance and other investigative work; and, finally, to create a strengthened state of alert.

No one will ever know what might have happened if more connections would have been drawn between the different pieces of information. It will never definitively be known to what extent the Community would have been able and willing to exploit fully all the opportunities that may have emerged.

4.5 INTELLIGENCE TODAY

Throughout all the history of America, intelligence helped to protect the U.S. country and its liberties. During such evolution, the U.S. took advantage from both the Constitution and traditions of limited government. The U.S. intelligence agencies were still using the U.S. system of checks and balances.

The new threats were made stronger thanks to the globalization and the Internet. With the 9/11 events, the Americans realized that it was time to adapt to a world where a bomb could be easily built in a basement. The missed signs that led to the U.S. attacks shook the country. What emerged was the desire and request that the intelligence community improved its capabilities, and that law enforcement changed practices in order to focus more on the prevention of attacks rather than on the prosecution of terrorists after an attack.

It is not easy to describe the transformation that the America's intelligence community faced after 9/11. Suddenly, the agencies were asked to do more than just monitoring hostile powers and obtaining information for policymakers; they had also to identify and target plotters in some of the most remote places of the world, and to anticipate the networks actions.

Today, the new capabilities help intelligence agencies in many ways, they allow to track terrorists contacts, and their moves. Information are collected and shared more quickly between federal agencies, and state and local law enforcement, thanks to the new laws.

By the time that President Obama took office "some of the worst excesses that emerged after 9/11 were limited through a combination of action by the courts, increased congressional oversight, and adjustments by the previous Administration."[128] But many different factors have continued to complicate the efforts to defend America and support its civil liberties.

[128] Obama's Speech on NSA Surveillance Reform, 17th January 2014, available at http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html

In a speech at the National Defense University in May 2013 President Obama suggested the need of a more robust public discussion with regard to the balance between security and liberty.

> *I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it in their own hands to publicly disclose classified information, then we will never be able to keep our people safe, or conduct foreign policy.*[129]

What the U.S. has to do is to take some important decisions about how to protect itself and sustain its leadership in the world, without forgetting to support the civil liberties and privacy protections required by its ideals.

President Obama's Speech about U.S. intelligence practices

During the last months, President Obama created an outside Review Group on Intelligence and Communications Technologies with the aim to make recommendations for reform. He has consulted with the Privacy and Civil Liberties

[129] Ibid

Oversight Board, listened to foreign partners, privacy advocates, and industry leaders. His Administration has worked at how to approach intelligence in this era of threats that are always more widespread and where technology is in constant revolution. This process of review has given some clear direction for change, as President Obama has pointed out.

> *First, I have approved a new presidential directive for our signals intelligence activities, at home and abroad. This guidance will strengthen executive branch oversight of our intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of America's companies; and our commitment to privacy and basic liberties.*
>
> *Second, we will reform programs and procedures in place to provide greater transparency to our surveillance activities, and fortify the safeguards that protect the privacy of U.S. persons. To ensure that the Court hears a broader range of privacy perspectives, I am calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.*
>
> *Third, we will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security.*
>
> *Fourth, in investigating threats, the FBI also relies on National Security Letters, which can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation.* [130]

This leads to the program that brought a great controversy during the last months: the bulk collection of telephone records under Section 215. Such program will not involve the content of phone calls or the names of people making calls but rather, it will record phone numbers and the times and lengths of calls. These records will be then collected into a database that the government will request if it has a specific suspect.

[130] Ibid.

The Review Group suggested a replacement of the current approach with one in which the providers or a third party keep the bulk records, letting the government have access to information as needed. As President Obama said:

> *The reforms I'm proposing today should give the American people greater confidence that their rights are being protected, even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe. I recognize that there are additional issues that require further debate.*[131]

U.S. capabilities will help to protect not only its nation, but also its friends and allies. The effectiveness of such efforts will depend on the degree of confidence of ordinary citizens in other countries that the United States respects their privacy too.

For this reason, the new directive of the president that has been issued on the 17 of January will clearly prescribe what is done, and what is not done. The directive will make it clear that the United States only use signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary people.

"In the terms of bulk collection of signals intelligence, U.S. intelligence agencies will only use such data to meet specific security requirements."[132] What the U.S. wants to do is to let other countries know that it is not spying ordinary people who don't threaten national security. Intelligence agencies will continue to obtain information about the intentions of governments around the world, in the same way that the intelligence services of every other nation do.

To make sure that they will follow through on these reforms, President Obama is making some important changes to the organization of the government.

[131] Ibid.
[132] Ibid.

4.6 THE FUTURE OF THE U.S. INTELLIGENCE

The Intelligence Community will continue to improve intelligence integration in order to use a more efficiently and effectively way the strengths and capabilities that are spread across its 17 organizations. Thanks to National Intelligence Managers and their associated Unifying Intelligence Strategies, the Director of National Intelligence has drawn together the expertise required to accomplish the tasks of the National Security Strategy and the National Intelligence Strategy. The Intelligence Community is working to ensure that integrated intelligence information will flow anywhere and at anytime any authorized user will require it.

The Intelligence Community continues with its investments to combat terrorism and support the Administration's National Strategy for Counterterrorism. It will continue to lead operations to defeat al-Qaeda and other violent extremists and disrupt their capabilities; prevent the proliferation of weapons of mass destruction; penetrate and analyze the most difficult targets of interest to U.S. foreign policymakers; identify and disrupt counterintelligence threats; and provide strategic warning to policymakers on issues of geopolitical and economic concern. In order to protect in a better way the national security, the IC will strengthen its collection and analysis capabilities and promote responsible intelligence collaboration and information sharing.

The Budget is an important factor that supports the ability of the Intelligence Community to play an important role in informing military decision-makers at the strategic level, as well as those on the ground. The Budget balances its focus between current, immediate needs for U.S. military forces engaged in operations with enduring intelligence requirements for potential future military and security needs.

Cyber threats are constantly evolving and require a coordinated and comprehensive way of thinking about cyberspace activities.

As long as the Intelligence Community continues to see across its Nation, no sector, network, or system will be immune from penetration by those who seek to

make financial gain, to perpetrate malicious and disruptive activity, or to steal commercial or government secrets and property.

The Budget includes increases and improvements to a full range of cyberspace activities. Moreover, the Budget supports the Senior Information Sharing and Safeguarding Steering Committee that were established by the President with the Executive Order 13587 to guide and prioritize Government-wide investments in classified networks and to support the Administration's National Strategy for Information Sharing and Safeguarding. The Budget continues to support the protection of these critical networks that facilitate the Intelligence Community's information sharing and operational requirements.

The Intelligence Community depends on information technology capabilities to support operations and allow for information sharing and collaboration with all authorized users. A modernization of this infrastructure will develop efficient solutions to the challenges of the IC's storage and data handling.

We still don't have any in-depth study of the discourse of intelligence, though the link between intelligence failures and such conceptual traps as mirror imaging and worst-case analysis have been identified.[133] An interesting way for exploration has been suggested by the concept of "chaos", as recently applied to international politics. Chaos theory suggests that intelligence services live in an indeterminate and unpredictable world.

Whether to avoid the worst of misunderstandings, or to engage in something more positively ambitious, intelligence has without any doubts a future, a future secured on the basis of the forward-thrusting revolution and on an accumulative historical precedent that has cemented the identification of intelligence and national security. What intelligence services are going to do will depend on the nature of change that can only be glimpsed, but that are already under way in the basic definitions of national security.

[133] A valuable study of intelligence failure is Richard K. Betts's "Analysis, War and Decision: Why Intelligence Failures are Inevitable", World Politics XXXI October 1978, pp. 61-90

In the future, national security will not mean simply the security of nation-state but it will instead mean the security of a pluralized system of governance, across which citizens will be likely to spread their loyalties and appeal for safety.

BIBLIOGRAPHY

BOOKS AND VOLUMES

- AMY ZEGARD, *Flawed by Design: The Evolution of the CIA, JCS, and NSC,* Stanford CA, Stanford University Press, 1999

- CYNTHIA M. GRABO, *Anticipating Surprise: Analysis for Strategic Warning*, 2002

- DARRIC MILLIGAN et al., *Intelligence –Led Policing Technology for State and Local Law Enforcement Agencies,* Bedford MA, Mitretek Corporation, MTR-2006-016, 2006

- DAVID WEISBURD and ANTHONY A. BRAGA (eds.), *Police Innovation: Contrasting Perspectives,* Cambridge, Cambridge University Press, 2006

- GREGORY F. TREVERTON, Intelligence for an Age of Terror, Cambridge University Press, 2009

- GREGORY F. TREVERTON, *Reshaping National Intelligence for an Age of Information*, Cambridge, Cambridge University Press, 2001

- JOE KLEIN, *Closework: Why We Couldn't See What Was Right in Front of Us,* The New Yorker, October 1, 2001

- JAY DAVIS, *Epilogue: A Twenty-First Century Terrorism Agenda for the United States,* in *The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors,* James M. Smith and William C. Thomas eds., 2001

- JERRY H. RATCLIFFE, “Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice”, *Policing and Society, 12,* 1, 2002

- JOHN LE CARRÉ, *The Night Manager,* New York, Knopf, 1993

- JOHN YOO*, The Power of War and Peace: The Constitution and Foreign Affairs After 9/11,* Chicago, University of Chicago Press, 2005

- JOHN YOO, *The Terrorist Surveillance Program and the Constitution*, George Mason Law Review, Vol. 14, 2007

- JONATHAN M. FREDMAN, *Intelligence, Law Enforcement, and the Prosecution Team,* Yale Law and Policy Review, Vol. 16, No. 2, 1998,

- JOSEPH NYE, *Speaking to the members of the Security Affairs Support Association*, Fort Meade, Md., April 24, 1993

- KARL WEICK, *Sense making in Organizations*, London, Sage Publications, 1995

- MARK M. LOWENTHAL, *Intelligence From Secrets To Policy*, CQ Press College, 2011

- MICHAEL SCHEUER, *Through Our Enemies’ Eyes: Osama Bin Laden, Radical Islam, and the Future of America*, 2002

- PETER BERKOWITZ, *The Future of American Intelligence,* Hoover Press, 2005

- RICHARD A. POSNER, *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11,* Rowman & Littlefield Publishers, Inc., 2005

- RICHARD K. BETTS, “Analysis, War and Decision: Why Intelligence Failures are Inevitable”, World Politics XXXI October 1978

- RICHARD L. DAFT and KARL E. WEICK, Toward a Model of Organizations as Interpretation Systems, Academy of Management, The Academy of Management Review, 1984

- RICHARD L. RUSSELL, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right,* Cambridge, Cambridge University Press, 2007

- ROBERTA WOHLSTETTER, *Pearl Harbor: Warning and Decision*, Stanford University Press, Stanford, CA, 1962

- SPENCER C. TUCKER, Vietnam, University Press of Kentucky, 1999

- STEELE R. D., *Intelligence – Spie e Segreti in un Mondo Aperto,* Rubbettino, Soveria Mannelli, 2002

DOCUMENTS

- *A review of the FBI's Handling of Intelligence Information Related to September 11 Attacks*, November 2004 source: *http://www.justice.gov/oig/special/s0606/final.pdf*

- *Attempted Terrorist Attack on Northwest Airlines Flight 253*, Report of the Select Committee on Intelligence United States Senate, 2010 source: *http://www.intelligence.senate.gov/pdfs/111199.pdf*

- Commission on the Roles and Capabilities of the U.S. Intelligence Community, Aspirin-Brown Commission, *Preparing for the 21st century: An Appraisal of U.S. Intelligence, Executive Summary*, Washington D.C., U.S. Government Printing Office, 1996

- *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate,* 94th Congress, 2nd Session, 1976, Book II, *Intelligence Activities and the Rights of Americans,* source: *http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm*

- *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate,* 94th Congress, 2nd Session, 1976, Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans,* source: *http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm*

- *Final Report,* Part I, the Joint Inquiry, December 10, 2002 source: *http://www.intelligence.senate.gov/press/findings.pdf*

- *Foreign Intelligence Surveillance Act of 1978*, Pub. L. No. 95-511, 92 Stat. 1783, source: *http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf*

- George W. Bush, *Graduation Speech at West Point*, 1 June 2002 source: *http://georgewbushwhitehouse.archives.gov/news/releases/2002/06/20020601-3.html*

- George W. Bush*, National Security Strategy of the United States of America*, Washington DC, September 2002 source: *http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA407178*

- *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures* (February 2003) source: *http://www.fas.org/irp/congress/2003_rpt/fisa.html*

- James G. March and Johan P. Olson, *Organizing Political Life: What Administrative Reorganization Tells Us about Government*, 1983, American Political Science Review, 77

- Laurie E. Ekstrand, *FBI Transformation: FBI Continues to Make Progress in Its Efforts to Transform and Address Priorities,* U.S. General Accounting Office GAO-94-578T, 2004

- Michael E. O'Hanlon, Susan E. Rice, and James B. Steinberg, "*The New Security Strategy and Preemption*," Policy Brief #113, December 2002 source:

http://www.brookings.edu/research/papers/2002/12/terrorism-ohanlon

- *National Counterterrorism Center*, Executive Order 13354, August 27, 2004, source: *http://www.gpo.gov/fdsys/pkg/CFR-2005-title3-vol1/html/CFR-2005-title3-vol1-eo13354.htm*

- Obama's Speech on NSA Surveillance Reform, 17th January 2014 source: *http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html*

- Richard A. Best Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS Report for Congress, Updated December 3, 2001

- Richard A. Best Jr., *The National Counterterrorism Center (NCTC)-Responsibilities and Potential Congressional Concerns,* December 19, 2011, source: *http://www.fas.org/sgp/crs/intel/R41022.pdf*

- Roger Z. George, *Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm*, source: *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html*

- Senator Richard Shelby's long supplementary document, *September 11 and the Imperative of Reform in the Intelligence Community, Additional Views,* December 10, 2002

- *Strengthened Management of the Intelligence Community*, Executive Order 13355, August 27, 2004, p. 1699 source:

  http://www.gpo.gov/fdsys/pkg/WCPD-2004-08-30/pdf/WCPD-2004-08-30-Pg1699.pdf

- The *Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC 2005

- The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report,* Washington DC 2004

- U.S Department of Homeland Security, *Implementing the 9/11 Commission Recommendations*, Progress Report 2011 source: *http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf*