NAVAL

POSTGRADUATE

SCHOOL

MONTEREY, CALIFORNIA

THESIS

ORGANIZING THE COUNTER TERRORISM UNIT OF THE REPUBLIC OF MAURITIUS: USING THE MAIN COUNTERTERRORISM AGENCIES OF THE UNITED STATES OF AMERICA AS MODELS

by

Rajcoomar Seebah

December 2011

Thesis Advisor:	Erik Dahl
Second Reader:	Maria Rasmussen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Organizing the Counter Terrorism Unit of the Republic of Mauritius: Using the Main Counterterrorism Agencies of the United States of America as Models		**5. FUNDING NUMBERS**	
6. AUTHOR Rajcoomar Seebah			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Mauritius Police Force or the Government of the Republic of Mauritius. IRB Protocol Number: N/A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT

In response to the rise of terrorism in the South West Indian Ocean and its potential to threaten national stability and security, the government of the Republic of Mauritius recently established a Counter Terrorism Unit (CTU) under the supervision of the National Counter Terrorism Committee (NCTC). This thesis examines the challenges involved in organizing this unit, whose mission is to collect and analyze all terrorism-related intelligence, and ultimately disseminate the finished product to the country's law and order apparatus. Setting up this agency is vital for integrating all national counter terrorism efforts and strategies to combat terrorism. However, this laudable effort to make the Republic of Mauritius more resilient to the threat posed by terrorism will require significant legal and organizational changes. This thesis examines similar organizations in the United States and elsewhere in order to develop lessons learned and best practices that can be applied in Mauritius. This study finds there will be a need to pool all available resources and bring multiple strands of expertise under one roof in a judicious mix of the state's defense, diplomatic, intelligence and law-enforcement capabilities.

14. SUBJECT TERMS Information sharing, interagency cooperation, counterterrorism.			**15. NUMBER OF PAGES** 93
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ORGANIZING THE COUNTER TERRORISM UNIT OF THE REPUBLIC OF MAURITIUS: USING THE MAIN COUNTERTERRORISM AGENCIES OF THE UNITED STATES OF AMERICA AS MODELS

Rajcoomar Seebah
Superintendent of Police, Mauritius Police Force
B.S., University of Mauritius and University of Portsmouth, U.K., 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(COMBATING TERRORISM: POLICY & STRATEGY)

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Rajcoomar Seebah

Approved by: Professor Erik Dahl
Thesis Advisor

Professor Maria Rasmussen
Second Reader

Professor Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In response to the rise of terrorism in the South West Indian Ocean and its potential to threaten national stability and security, the government of the Republic of Mauritius recently established a Counter Terrorism Unit (CTU) under the supervision of the National Counter Terrorism Committee (NCTC). This thesis examines the challenges involved in organizing this unit, whose mission is to collect and analyze all terrorism-related intelligence, and to disseminate the finished product to the country's law and order apparatus. This agency will be vital for integrating national counter terrorism efforts and strategies. However, this laudable effort to make the Republic of Mauritius more resilient to the threat posed by terrorism will require significant legal and organizational changes. This thesis examines similar organizations in the United States and elsewhere in order to develop lessons learned and best practices that can be applied in Mauritius. This study finds there will be a need to pool all available resources and bring multiple strands of expertise under one roof in a judicious mix of the state's defense, diplomatic, intelligence and law-enforcement capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASIO	Australian Security Intelligence Organization
ATF	Bureau of Alcohol, Tobacco and Firearms
CIA	Central Intelligence Agency
CTIUs	Counter Terrorism Intelligence Units
CTU	Counter Terrorism Unit
DEA	Drug Enforcement Administration
DG	Director General
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DoE	Department of Energy
DS	Directorate of Support
DS&T	Directorate of Science and Technology
DST	Direction de la Surveillance du Territoire
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
GCHQ	Government Communications Headquarters
GIGN	Groupe d'Intervention de la Gendarmerie Nationale
GIPM	Groupe d'Intervention de la Police Mauricienne
HPSCI	House Permanent Select Committee on Intelligence
IGIS	Inspector General of Intelligence and Security
INR	Bureau of Intelligence and Research
JTTF	Joint Terrorism Task Force
KGB	Soviet Komityet Gosudarstvennoy Bezopasnosty
MI5	Military Intelligence Group 5
MPF	Mauritius Police Force

NCIS	Naval Criminal Investigative Service
NCIX	National Counterintelligence Executive
NCPC	National Counterproliferation Center
NCS	National Clandestine Service
NCTC	National Counter Terrorism Committee
NCTC	National Counter Terrorism Center
NGA	National Geospatial-Intelligence Agency
NIC	National Intelligence Council
NIEs	National Intelligence Estimates
NIOs	National Intelligence Officers
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NYPD	New York Police Department
ONSI	Office of National Security Intelligence
PHQ	Police Headquarters
PJCIS	Parliamentary Joint Committee on Intelligence and Security
RPA	Radiation Protection Authority
SIS	Secret Intelligence Service
SSCI	Senate Select Committee on Intelligence
SWAT	Special Weapons and Tactics
U.K.	United Kingdom
U.S.	United States
U.S.C.G.	United States Coast Guard
WMD	Weapons of Mass Destruction

EXECUTIVE SUMMARY

In recent decades, scientific progress and the effects of globalization have had significant impact on our daily life. However, these changes are a mixed blessing, with far reaching effects and unimagined consequences. While innovations in technology, communication, and transportation contribute to improvements in our standard of living and facilitate our day-to-day activities, progress has also created a borderless network of highly motivated adversaries–terrorists–who act unpredictably and with increasing levels of ferocity around the world. Consequently, terrorism has today become a major concern to all governments and poses a significant threat to our values and way of life. Because terrorist attacks are unpredictable, governments must act proactively to afford a safe and secure environment for law-abiding peace loving communities.

The government of the Republic of Mauritius is much attuned to the omnipresent threats from terrorism, such as those resulting from open and direct air access to many countries where terrorist activities already exist. Though the Republic of Mauritius is arguably more secure than most countries in the Indian Ocean, the nation has nonetheless taken preventive measures to mitigate the terrorist threat. In the aftermath of the September 11, 2001 terrorist attacks in the United States, a National Counter Terrorism Committee (NCTC), chaired by the Secretary for Home Affairs, was established at the level of the Prime Minister's office to review national counterterrorism measures on a regular basis. The latest development is the establishment of the Counter Terrorism Unit (CTU) in 2009, tasked with collecting and analyzing all terrorism-related intelligence, and ultimately disseminating the finished product to the country's law and order apparatus. This unit is still at its inception stage. Once it is fully operational, it will function under the supervision of the National Counter Terrorism Committee, and will be directly responsible to the Prime Minister. This thesis examines the organizational and policy challenges that the CTU will face, and examines similar organizations in the United States and elsewhere in an effort to develop lessons learned and best practices that can be applied by the government of Mauritius.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The fifteen months that I have spent at the Naval Postgraduate School have been instrumental for the realization of this thesis. I would therefore like to thank all the professors of the Department of National Security Affairs for their valuable contributions.

To my thesis advisor, Professor Erik Dahl, I extend my deepest gratitude and appreciation for his continuing concern, guidance, and support throughout the thesis process and for arranging the meeting with the Deputy Director of the Northern California Regional Intelligence Center in San Francisco. I would also like to thank Professor Maria Rasmussen, my second reader, for her advice in editing and shaping this thesis.

I further convey my sincere thanks to Capt. Jennith Hoyt, Senior Intelligence Officer, and Commander Tim Unrein, Director of the Information Dominance Center for Excellence at the Naval Postgraduate School, for setting up the meetings with the professionals of the U.S. intelligence community in Washington D.C. My appreciation also goes to Mr. Randy Burkett, DCIA representative, and Special Agent Mary C. Teer from the Naval Criminal Investigative Service at the Naval Postgraduate School for arranging the meeting with the Joint Terrorism Task Force in San Francisco.

A special note of thanks to Mr. Mike Sena, Deputy Director of the Northern California Regional Intelligence Center, Mr. Bill Buchalter, Senior Officer of the Joint Terrorism Task Force in San Francisco, Professor Paul Shemella from the Center for Civil-Military Relations at the Naval Postgraduate School, Mr. Paul Abbate, Section Chief of the Counterterrorism Division of the Federal Bureau of Investigation in Washington D.C., Commander Eric Borio, Division Chief of the Directorate of Intelligence and Information Sharing of the Naval Criminal Investigative Service in Quantico, and Capt. Peter J. Hatch, Commanding Officer of the U.S.C.G. Intelligence Coordination Center in Suitland, for sharing their experience and expertise on interagency cooperation and the organizational structure of intelligence agencies.

And lastly, I dedicate this thesis to my wife Sheila, and my two sons, Yoann and Kenan, who have been very cooperative and understanding.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Republic of Mauritius is a multi-ethnic society divided by religion, caste, language, and ethnicity. The main communities are the Hindu descendants of indentured laborers who originated from India, Creole descendants of African slaves, Indo-Muslims from western and northern India, Tamils from Southern India, Chinese, and a minority of European ethnic communities—French, British, and Dutch. It is an island which occupies a key strategic location in the Southern Indian Ocean, with an Exclusive Economic Zone of 1.9 million square kilometers.

The country is renowned as an island paradise where tourists enjoy peace, calm and security. However, the island is located in the midst of some major cross-currents in international terrorism. There are established linkages between Tanzania, South Africa, and other countries of sub-Saharan Africa on the one hand, and terrorist hubs located in the Pakistan-Afghanistan region on the other. The ideological wellsprings of Salafism in West Asia are not far away. Nearer home, major sea lanes and maritime traffic in our vicinity remain potential targets. A robust democracy, advanced technology, vibrant tourist industry, good telecommunications, and offshore banking make Mauritius a potential area of interest for forces who may be tempted to use our open and free society to disrupt peace and threaten our prosperity. Indeed, though the Republic of Mauritius has not been home to incidents of such magnitude, globalization makes the threat of terrorism omnipresent. The November 2008 terrorist attack in Mumbai, India, is a bitter and harsh reminder of this fact. However, the Republic of Mauritius has always been proactive in mitigating the threats from terrorism.

A. COUNTERTERRORISM MEASURES

Since independence in 1968, the Republic of Mauritius has taken a number of steps to align itself with efforts in other countries to mitigate the effects of terrorism. Indeed, it has enacted a number of laws criminalizing terrorist acts and terrorist-related activities, entered regional and international agreements for the war against terror, and developed a variety of internal mechanisms to combat terrorism.

1. Legal Framework

The government of Mauritius has passed a number of laws to support the counterterrorism efforts of the country.[1] These include the following:

- Extradition Act 1970
- Immigration Act 1970
- Continental Shelf Act 1982
- Explosives Act 1982
- Civil Aviation (Hijacking and Other Offences) Act 33 of 1985.
- Banking Act 1988
- Stock Exchange Act No 38 of 1988
- Unit Trusts Act No 26 of 1989
- Customs Acts 1989
- Insurance (Amendment) Act No 22 of 1990
- Foreign Exchange Dealers Act 1995
- Securities (Central Depository, Clearing and Settlement) Act 1996
- The Dangerous Drugs Act 2000
- Financial Services Development Act 2001
- Trusts Act No 14 of 2001
- Prevention of Terrorism Act 2002
- Prevention of Corruption Act 2002
- The Financial Intelligence and Anti-Money Laundering Act 2002

[1] Laws of Mauritius, http://www.gov.mu/portal/site/GovtHomePagesite/menuitem.c0a01177fcf48dfcf6be501054508a0c/?content_id =8b4484d776e98010VgnVCM100000ca6a12acRCRD (accessed Oct 29, 2011).

- The Financial Intelligence and Anti-Money Laundering Regulations 2003
- The Anti-Money Laundering (Miscellaneous Provisions) Act 2003
- Prevention of Terrorism Act (Special Measures) GN 14 of 2003
- The Dangerous Drugs (Amendment) Act 2003
- The Geneva Conventions Amendment Act 2003
- The Chemical Weapons Convention Act 2003
- The Radiation Protection Act 2003
- The Computer Misuse and Cybercrime Act 2003
- The Convention for the Suppression of Financing of Terrorism Act 2003
- Mutual Legal Assistance in Criminal and Related Matters Act 2003
- Financial Reporting Act No 45 of 2004
- Data Protection Act No 13 of 2004
- Biological and Toxin Weapons Convention Act 2004
- Dangerous Chemical Control Act 2004
- Banking Act 2004
- Bank of Mauritius Act 2004
- Firearms Act 2006
- Prevention of Terrorism (International Obligations) Act 41 of 2008

2. International and Regional Cooperation

The Republic of Mauritius belongs to various international and regional security organizations. It has adopted a number of conventions and resolutions and has contracted partnership agreements to show its commitment to addressing all forms and manifestations of terrorist threats.

As a member of the United Nations, the Republic of Mauritius is a signatory to the following legal documents:

- United Nations Security Council Resolution 1373
- UN Convention for the Suppression of Terrorist Bombing 2003
- UN Convention Against Transnational Organized Crime 2003
- UN Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons 2003
- International Convention for the Suppression of Acts of Nuclear Terrorism 2005

As part of the South African Regional Police Chiefs Cooperation Organization, the Republic of Mauritius actively shares information with member states to prevent cross border crime. And as a member of the African Union, the Republic of Mauritius signed and ratified the 1999 African Union Convention on the Prevention and Combating of Terrorism and contributes to the African Centre for the Study and Research on Terrorism, established in Algiers in 2004 as to raise the African Union's capacity to prevent and combat terrorism in Africa. Lastly, the government of Mauritius signed a Memorandum of Understanding with the government of India in 2008 to facilitate the exchange of information relating to money laundering and terrorist financing.

3. Internal Structures

The country started developing the operational component to respond to terrorism threats in the early 1980's. At first, with the assistance of the French government, it set up a tactical unit as the strike force for counter terrorism operations, the *Groupe d'Intervention de la Police Mauricienne* (GIPM), which replicates the French *Groupe d'Intervention de la Gendarmerie Nationale* (GIGN). Later, the government created the Radiation Protection Authority (RPA) in 2006, upon proclamation of the 2003 Radiation Protection Act. The RPA, under the aegis of the Ministry of Energy and Public Utilities, deals with the regulation, control, and supervision of radiological activities related to the acquisition, importation, use, transportation and disposal of radioactive material, radioactive substances, x-ray equipment, and other sources of ionizing radiation. In the

aftermath of the September 11, 2001, terrorist attacks in the United States, a National Counter Terrorism Committee, chaired by the Secretary for Home Affairs, was set up at the level of the Prime Minister's Office to review the country's counterterrorism measures on a regular basis. The latest development is the establishment of the Counter Terrorism Unit (CTU), charged with collecting and analyzing all terrorism-related intelligence, and ultimately disseminating the finished product to the country's law and order apparatus. The CTU functions under the supervision of the National Counter Terrorism Committee (NCTC), and is directly responsible to the Prime Minister.

B. MAJOR RESEARCH QUESTION

The aim of this thesis is to explore how the CTU is best organized to effectively fulfill its mission, which is to proactively combat all forms of terrorism in order to make the Republic of Mauritius more resilient to terrorism. This study addresses issues pertaining to the type of network needed for effective collection, sharing and dissemination of intelligence among the relevant agencies in the int**e**lligence community. The thesis also investigates the practices that should be adopted by the CTU to ensure that the unit operates within the parameters of the rule of law and without infringing on civil liberties.

C. PROBLEMS

At the outset, it seems likely that the two main problems in developing the CTU of the Republic of Mauritius will be information sharing between agencies in the intelligence community and the challenges to intelligence collection with regard to civil liberties.

1. Lack of Interagency Cooperation

Unlike the United States, with its National Security Act of 1947 and Intelligence Reform and Terrorism Prevention Act of 2004, the Republic of Mauritius has no official legal document specifying the agencies that comprise the intelligence community. While some intelligence agencies are part of the Mauritius Police Force, which is under the central command of the Commissioner of Police, the others are controlled by various

government ministries. Given this context, there will be a need to address issues of interagency coordination and cooperation to set up an intelligence sharing network to facilitate effective, efficient, and timely responses in the fight against terrorism.

2. Effect of Intelligence Activities on Civil liberties

The nation's strong civil society places a lot of emphasis on the protection of civil liberties and compliance with the rule of law by enforcement agencies. Consequently, intelligence agencies will have to project legitimacy in order to win the trust of the population. It is argued that legitimacy can only be achieved with proper oversight of intelligence agencies and appropriate mechanisms to ensure that they operate within legal parameters and in strict compliance with the rule of law.

D. LITERATURE REVIEW

Intelligence is a key factor in countering terrorism as it can provide the means to anticipate, pre-empt, and respond to this threat.[2] Generating actionable intelligence for effective, efficient, and timely responses is a cycle which involves several processes, including collection and analysis of raw information. However, the cycle is incomplete if intelligence is not properly shared. From this perspective, it can be argued that the failure of the intelligence community to respond to terrorist attacks can be attributed to failures in any of these three processes–collection, analysis, or sharing.

To substantiate this argument, the first part of this literature review analyzes the arguments posited as the main causes of failure within the intelligence community by the three main schools of thought—the orthodox school, the intelligence reformist school and the Central Intelligence Agency critics' school.[3] In the second part, I argue that factors such as competing interests, organizational culture, technical incompatibilities, and the absence of a coordinating body can act as obstacles to cooperation or "firewalls" between agencies of the intelligence community.

---

[2] Bruce Hoffman, "Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post Cold War Era,*" Intelligence and National Security* 11, no. 2 (1996): 219.

[3] Erik J. Dahl, "Intelligence and Terrorism," in Robert Denemark et al., eds., The International Studies Encyclopedia, part of the *International Studies Association Compendium Project* (Oxford: Wiley-Blackwell, 2010), 3862–3882.

1. Theoretical Perspectives

Dahl argues that in the aftermath of the 9/11 attacks, three main schools of thought have emerged to explain the intelligence community's failure to significantly impact the threat posed by terrorism. This section reviews each of these schools of thought, and considers what the analysis of each school would imply for the development of the CTU in Mauritius.

a. Orthodox School

The proponents of this school of thought adopt a very pessimistic approach, arguing that intelligence failures are bound to happen and that nothing can be done to prevent their occurrence as they are difficult to predict.[4] They advocate that the best course of action is to develop plans to deal with the effects of terrorist attacks.[5] They claim that surprise attacks are more likely if those responsible for decision making in the fight against terrorism disregard the warnings of the intelligence community.[6] However, they admit that there is fierce competition for the attention of policy makers, in the massive amount of intelligence about a wide range of threats, as well as between such threats and other pressing policy issues.[7] When there is a multitude of dots, the number of ways to connect the dots increases, adding more complexity to already complex issues.[8]

This school of thought offers few lessons that can be used in the establishment of a new CTU. The goal of the new unit is to prevent terrorist attacks wherever possible. Because the orthodox school believes that prevention is very difficult, we must look elsewhere for useful advice and suggestions for accomplishing a mission of prevention.

---

[4] Richard A. Posner, *Countering Terrorism: Blurred Focus, Halting Steps* (Lanham, MD: Rowman and Littlefield, 2007), 23.

[5] Dahl, "Intelligence and Terrorism," 3869.

[6] Ibid.

[7] Ibid., 3870.

[8] Richard K. Betts, *Enemies of intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), 105.

b. Intelligence Reformist School

The scholars and analysts of the intelligence reformist school are less pessimistic than their orthodox counterparts. They claim that failures occur because of the lack of communication between agencies of the intelligence community, and this lack of communication is due to organizational structure.[9] Zegart argues that counterterrorism efforts are less effective when there is no central mechanism with a common strategy to coordinate agencies that are often scattered and underfunded.[10] The intelligence reformist school argues that the analytical processing of information is not assigned enough importance, and the imagination to make sense of information already at hand is lacking.[11] In this context, Dahl argues that very often too much emphasis is laid on developing tactical level intelligence which is not adequate for generating the strategic-level intelligence assessments required by current threats.[12]

This school of thought suggests that interagency cooperation and coordination among agencies, as well as in-depth analysis of information, are important factors that the Counter Terrorist Unit of the Republic of Mauritius Unit should consider to support its ability collect information and produce actionable intelligence.

c. Central Intelligence Agency Critics' School

The third school of thought was developed and named following scholarly analysis of the responsibilities of the Central Intelligence Agency in the September 9/11 attacks. It argues that the success of terrorist attacks can be attributed to inadequate strategies for dealing with a phenomenon unlike the type of threat we were used to in the past.[13] As a remedy to this problem, Jenkins supports building up the institutional

---

[9] Dahl, "Intelligence and Terrorism," 3869–3871.

[10] Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007), 3.

[11] Dahl, "Intelligence and Terrorism," 3869–3870.

[12] Ibid., 3870.

[13] Ibid., 3869.

intelligence capabilities of the intelligence community to collect information, and argues that more focus should be put on human intelligence and intelligence units at the local level.[14]

The lessons from this school of thought for Mauritius are very enriching. From this perspective, it is worthwhile for the CTU to consider using or tapping into the Mauritius Police Force's existing information collection network.

2. Obstacles to the Intelligence Cycle within the Intelligence Community

Interagency coordination and cooperation within the intelligence community in the fight against terrorism is a prerequisite for effective, efficient, and timely response. Factors such as competing interests, organizational culture, technical incompatibilities, and absence of a coordinating body can impede the creation of the conductive environment necessary for an effective intelligence sharing network.

a. Competing Interests

With limited resources, governments nowadays place increasing emphasis on performance-based budgeting in the public sector so as to more efficiently and effectively manage public expenditures.[15] Consequently, this increases the competition between the agencies of the intelligence community over finite governmental resources. Indeed, these agencies continuously strive to increase their visibility within the government sector, as higher visibility is synonymous with higher budget allocation. This has become a major obstacle to interagency cooperation, as there is less willingness to collaborate and to share information. Worse still, they are now competing against each other.[16]

---

[14] Brian Jenkins, "Statement to the National Commission on Terrorist Attacks Upon the United States," Washington (March 2003), http://govinfo.library.unt.edu/911/hearings1/witness_jenkins.htm. (accessed May 25, 2011).

[15] Marc Robinson, and Duncan Last, "A Basic Model of Performance-Based Budgeting," *International Monetary Fund,* (Sept 2009), 2.

[16] Lawrence E. Cline, "Interagency Decision Making," in *Civil-Military Responses to Terrorism* (Monterey, CA: Naval Postgraduate School, 2011), 1.

b. Organizational Culture

Each organization has its own set of values, beliefs, norms and practices developed over time that have worked well enough to be considered valid. An organizational culture determines how individuals within the organization behave and how they expect others to behave. More importantly, it drives the way the organization conducts business and interacts with the wider community.[17] It can be argued that organizational culture can hamper effective cooperation between agencies, as was pointed out in the 9/11 Commission Report. With time, an organizational culture can create an even more complex set of rules and encompass a wider set of beliefs that discourages agencies within the intelligence community from even seeking to share information.[18]

c. Technical Incompatibilities

Cline argues that differences in agencies' levels of sophistication, especially in technical matters, can act as a barrier to effective coordination.[19] In a number of countries, information sharing cannot be effected because of basic problems like incompatible computer operating systems or absence of common databases, issues that sometimes occur when agencies do not yet see technology as an important asset. Technical incompatibilities can be explained by the lack of common procedures for the acquisition of equipment, lack of resources, or simply some organizations' resistance to change.

d. Absence of a Central Coordinating Body

The intelligence community is composed of a multitude of agencies that often do not fall under the same department or chain of command. It is not uncommon to find that by virtue of their roles and responsibilities, these agencies occupy equal status in

---

[17] Amanda Sinclair, "Approaches to Organisational Culture and Ethics," *Journal of Business Ethics* 12, no. 1 (1993), 63–64.

[18] Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at http://govinfo.library.unt.edu/911/report/911Report.pdf (accessed May 25, 2011), 539.

[19] Cline, "Interagency Decision Making," 3.

the hierarchy. Thus, finding out who is in charge is problematic.[20] Under these circumstances, agencies are not bound to cooperate or share information unless there is a central body with the relevant legal provisions to act as the coordinating mechanism. It can be argued that this is a prerequisite for putting together the various pieces and strands gathered by individual agencies. Even more importantly, because the window of opportunity to respond to an imminent threat is very small, a coordinating mechanism is necessary for fast and effective decision making.

3. Conclusion

This literature review reveals that intelligence failures happen for a number of reasons: the difficulty of predicting terrorist attacks, the lack of interagency cooperation, insufficient emphasis on the analytical processing of information, and/or the reluctance of the intelligence community to focus more on human intelligence. Furthermore, the lack of communication between intelligence agencies due to organizational structure, technical incompatibilities or competing interests, along with the absence of a central mechanism for coordinating among agencies, can all increase the propensity for intelligence failures.

These observations motivate a systematic examination of an integrated model involving a judicious mix of the defense, diplomatic, intelligence and law-enforcement capabilities of the state. Pooling all available resources and drawing together multiple strands of expertise can remove the barriers to effective interagency cooperation so the dots can be connected more accurately. This model can be used to show how the CTU can be organized to most effectively collect, collate and analyze terrorism-related intelligence and disseminate the finished product to the nation's law and order apparatus.

E. METHODOLOGY AND THESIS OUTLINE

In the next chapter, I provide the theoretical background for the development of this thesis, identifying the main characteristics of intelligence services, the various steps of the intelligence process, and the legal framework and types of mechanisms (executive,

[20] Cline, "Interagency Decision Making," 4.

legislative, judicial, and internal) required to ensure that security intelligence agencies operate within a democratic framework and are accountable to the civil society.

I believe that the 9/11 Commission Report was instrumental in reshaping the United States intelligence community to improve the effectiveness of its response to terrorism. Many academic studies analyze the extent to which these recommendations have been put into practice and evaluate the effectiveness of these reforms. Because I am doing my master's degree in the United States, I have taken the opportunity to interact with the professionals in this field. Their practical experience and expertise adds value to this thesis. Accordingly, in the third chapter I analyze how the United States has restructured its intelligence community since the 9/11 attacks. Chapter III explores the office of the Director of National Intelligence, the three main categories of intelligence agencies and their various functional mission support units, in order to identify organizations that might serve as models for the Republic of Mauritius Counter Terrorism Unit.

In the fourth chapter, I analyze in depth the three main U.S. models of Counter Terrorism–the National Counter Terrorism Center, the Joint Terrorism Task Force and the Intelligence Fusion Centers–by focusing on their organizational structures, roles and responsibilities in order to identify key points that might be useful for organizing the CTU of the Republic of Mauritius.

In the last chapter, I focus on the implementation of the lessons learned in the previous chapters and through personal interactions with the Deputy Director of the Northern California Regional Intelligence Center, the Senior Officer of the Joint Terrorism Task Force in San Francisco, the Commanding Officer of the U.S.C.G. Intelligence Coordination Center in Suitland, the Section Chief of the Counterterrorism Division of the Federal Bureau of Investigation in Washington, D.C., and the Division Chief of the Directorate of Intelligence and Information Sharing of the Naval Criminal Investigative Service in Quantico. These meetings were organized by my thesis advisor in liaison with the International Program Office, the Naval Criminal Investigative Service, and the Information Dominance Center for Excellence at the Naval Postgraduate School.

II. THE ROLE OF INTELLIGENCE

Intelligence plays a fundamental role in the development of an effective counterterrorism strategy. Among other advantages, it can help identify individuals and groups engaged in terrorism as well as their locations and sources of recruitment. It enables security agencies to track down the suspects and their logistic and financial supports. In addition, intelligence provides advance warning of potential terrorist threats. It can provide tactical information for counterterrorism operations to disrupt terrorist activities and terrorist command and control structures. Lastly, it can aid management of an actual or potential crisis by providing decision makers with actionable intelligence.[21]

Accordingly, the collection and analysis of information have always been considered extremely valuable to states. The emergence of agencies to address national, regional, or international security issues is a common feature of many countries around the world, especially in the last century. Commonly referred to as intelligence agencies, these special organizations play an important role in providing states with the necessary intelligence[22] to make sense of their environment, assess present and potential adversaries,[23] avoid strategic surprises, provide long-term expertise, support the policy process, and maintain the secrecy of information, needs and methods.[24] However, it is important to note that the process of collecting raw information and converting it into actionable intelligence is part of larger cycle. In a democratic framework, intelligence gathering must be conducted in compliance with the rule of law to ensure that the civil rights of individuals are not violated. Indeed, there is a need for a democratic control so the roles and responsibilities of the intelligence community are directed by the civilian

---

[21] Anneli Botha, *Counterterrorism Training Manual* (Pretoria, SA: Institute for Security Studies, 2009), 209.

[22] "Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs." Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2009), 1.

[23] Robert Jervis, "Intelligence, Civil-Intelligence Relations, and Democracy," in Thomas C. Bruneau and Steven C. Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), vii.

[24] Lowenthal, *Intelligence: From Secrets to Policy*, 2.

authority, the parameters within which it operates are defined in law, and there are established procedures for reviewing issues such as use of resources and personnel management.[25] For example, in the U.S., a legal framework regulates the work of intelligence agencies and various control mechanisms ensure that they operate within a democratic framework.[26]

A. CHARACTERISTICS OF INTELLIGENCE AGENCIES

An analysis of intelligence agencies reveals that they share some common characteristics: adaptability, organizational structure, organizational command, relationship with the intelligence community, and a mechanism to ensure accountability. In this chapter, I analyze the development of intelligence services dealing with terrorism from France, England, and Australia to identify the important characteristics for developing a counter terrorism unit. These countries are chosen because of their relevance to the situation in Mauritius.

The Republic of Mauritius was a French colony from 1638 to 1810 and the French influenced the mode of operations and how the country deals with internal security issues. In the 1980s, the French government supported the government of Mauritius's establishment of response unit to deal with public order problems in general and terrorism in particular. This unit, known as the Mobile Wing, is under the command of the paramilitary unit of the country. The riot control component is organized and equipped along the same lines as the French *gendarmerie mobile*, while its counter terrorism component is a replica of the French *Groupe d'Intervention de la Gendarmerie Nationale* (GIGN), the counter terrorism strike force.

The present political and legal structures and law enforcement organizations of Mauritius, including the paramilitary, were significantly influenced by the British; Mauritius was a British colony from 1810 to 1968. The country adopted the Westminster model of government with a prime minister as the head of the Government. Court

[25] Thomas C. Bruneau and Steven C. Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," in Thomas C. Bruneau and Steven C. Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), 14.

[26] Ibid., 13–16.

procedures, criminal law, and laws of evidence are all derived from the British criminal justice system, as the country was policed under British law until independence. In addition, the paramilitary unit is structured on the same lines as the infantry battalions of the British Army.

Like the Republic of Mauritius, Australia is an island with a very diverse population, and both lie in the Indian Ocean. Both countries are presently very concerned with the emergence of extremists' jihadist networks that link militants in South East and South West Asia with the Middle East.

1. Adaptability

In France, the *Direction de la Surveillance du Territoire* (DST), set up during World War II, was responsible for gathering intelligence at the domestic level. Their focus was to identify Axis agents and collaborators. During the Cold War, their field of operation broadened. In addition to monitoring the threat posed by agents of the Soviet Komityet Gosudarstvennoy Bezopasnosty (KGB), the agency played an active role against the national insurgency in Algeria.[27] It is argued that the real shift of the DST to counter terrorism proper happened in the 1970's, when it confronted Carlos the Jackal and the Armenian Secret Army for the Liberation of Armenia. The DST became the principal agency monitoring threats from domestic Arab groups supported by Iran after the involvement of French forces in the first Gulf War and in Lebanon. Nowadays, the focus of the DST is on the threat posed by cells that are associated with the Al Qaeda network and to Al Qaeda for the Islamic Maghreb, which emerged from the Algerian Salafist Group for Prayer and Combat.[28]

In the United Kingdom, the Security Service, also known as MI5 (Military Intelligence, Group 5) was created in the early twentieth century attempted to mitigate the threat posed by Germany. Germany was conducting an espionage campaign in Britain aimed primarily at military targets and the British were concerned with a probable

[27] Brian A. Jackson, "Considering the Creation of a Domestic Intelligence Agency in the United States," *Rand* (2009), 67.

[28] Ibid., 72.

invasion. After World War II, the Security Service was given the primary responsibility for defense from acts of subversion aimed at overthrowing the government by unlawful means. MI5 continued to operate alongside the police Special Branches. The most significant change is the close relationship that developed between the security and intelligence agencies beginning in the late 1960s and early 1970s. With emerging threats of domestic and international terrorism, the Security Service started gathering intelligence on foreign nationals operating in the UK and members of terrorist organizations based abroad, in collaboration with other intelligence agencies including the Secret Intelligence Service (MI6), which is responsible for intelligence, and the Government Communications Headquarters (GCHQ), known as the signals intelligence agency.[29]

2. Organizational Tasks of Intelligence Agencies

The mission of advising the state after identifying and investigating threats to national security is the ultimate goal of all intelligence agencies. However, they also perform other tasks to make the country more resistant to terrorist attacks. For example, the primary task of the Australian Security Intelligence Organization (ASIO) is to produce tactical and strategic threat assessments on a regular basis. The focus of the former is on the probability that specific places, events, or categories of people will be targets of terrorist attacks. Strategic assessment, on the other hand, focuses on monitoring the evolution of regional and international terrorism and its probable impact on the country.[30]

The ASIO advises the private and public sectors on how to protect critical infrastructures through outreach programs designed to sensitize them to the risk of terrorist attacks. They have also set up a network for sharing classified materials with their partners to enhance the protection of their assets as well as the protection of those working in their organizations.[31]

---

[29] Jackson, "Considering the Creation of a Domestic Intelligence Agency in the United States," 118–120.

[30] Ibid., 16–17.

[31] Ibid., 17–18.

The ASIO is also responsible for vetting personnel who by virtue of their position will have access to sensitive information, as well as those who work in secured areas, like seaports and airports, or with access to dangerous explosive material.[32]

The ASIO plays an active role in border security by helping the immigration department exercise proper control over people entering the country. This is achieved with an up-to-date database of people deemed potential threats if allowed on the territory. It is also responsible for assessing people granted temporary protection visas and making recommendations for visa extensions.[33]

Lastly, the ASIO is the lead agency of a governmental consortium to prevent terrorists from developing weapons of mass destruction (WMD) using resources available in the country. It maintains a database on chemical, biological, radiological, nuclear and explosive terrorism and conducts regular assessments of the probability of terrorists using unconventional means to cause mass destruction.[34]

3. Organizational Command

Given the very small window of opportunity for effective response to imminent threats, intelligence agencies need a command structure that allows rapid decision making. The leadership of intelligence agencies needs access to the highest level government decision makers with the shortest possible delay and without having to go through the normal bureaucratic channels. For example, in the United Kingdom (UK), the Director General (DG) of the MI5 and the officers in charge of the other intelligence services have the right to direct access to the prime minister, who bears the overall responsibility for national security.[35] There is a need to ensure that those entrusted with such powers have the required expertise to shoulder their responsibilities and at the same time make judicious use of their power.

---

[32] Jackson, "Considering the Creation of a Domestic Intelligence Agency in the United States," 18.

[33] Ibid., 18.

[34] Ibid., 19.

[35] Ibid., 124–125.

It is important to note that while it is common practice in some countries for intelligence agencies to recruit the individual to head the organization from within their own agencies,[36] in some places there is a complete departure from this practice. For example, in Australia, the tendency is to recruit the Director General of the ASIO from outside the agency, to avoid the impression that it is a family business–old-boy inside trading[37]—and to prevent it from becoming a self-replicating bureaucratic structure.[38]

4. Relationship with Law Enforcement and Other Intelligence Agencies

Interagency coordination and cooperation within the intelligence community in the fight against terrorism is a prerequisite for effective, efficient, and timely response. A conducive environment is therefore of paramount importance in creating an intelligence sharing network. In the United Kingdom, the Security Service Act of 1989 and a number of ministerial guidelines enable the Security Service to collaborate closely with the Special Branches of the police forces at regional and local levels for counterterrorism activities.[39] From a structural perspective, the Security Service has a number of regional offices; the police have Counter Terrorism Intelligence Units (CTIUs) and Counter Terrorism Units (CTUs) at the regional level to facilitate the information gathering and intelligence sharing process.[40] The Security Service subsequently coordinates with the Secret Intelligence Service (SIS) and the GCHQ for an overall domestic and international threat analysis.[41]

5. Accountability and Oversight

Intelligence agencies rely a lot on people in order to fulfill their mission, and people are among their most important sources of information. Consequently, it is absolutely necessary that these agencies project legitimacy and trust to ensure effective

---

36 Jackson, "Considering the Creation of a Domestic Intelligence Agency in the United States," 125.

37 Ibid., 24–25.

38 Ibid., 25.

39 Ibid., 130.

40 Ibid., 131.

41 Ibid., 129.

cooperation with the population. This requires proper oversight of intelligence agencies and guarantees that they will operate legally and in accordance with the rule of law. For example, in Australia, the roles and functions of the ASIO are overseen by the Inspector General of Intelligence and Security (IGIS) and the Parliamentary Joint Committee on Intelligence and Security (PJCIS).[42] The former can access organizational staff and documentation in order to investigate the legal compliance of both past and current operations.[43] The latter has the authority to investigate matters pertaining to the administration and expenditures of the ASIO.[44]

B. THE INTELLIGENCE PROCESS

Johnson argues that intelligence as a term can be defined from two different perspectives. It can refer to the knowledge and foreknowledge of the world that state level decision makers need to make strategic decisions. It can also refer to specific conditions in a particular theatre, such as a battlefield, at a specific period of time.[45] Though both approaches are relevant, this thesis focuses on the strategic perspective because the role of the CTU is to inform the government of Mauritius about threats from domestic and international terrorism.

Even from this perspective, intelligence can further be defined in four different ways. Firstly, it can refer to information at the domestic and international levels that should be collected and analyzed to assist policy makers' understanding of the political, economic, social, and military environment.[46] Secondly, it can be thought of as a sequence of steps that starts with requirements by decision makers for information on specific issues and includes the process by which this information is collected, analyzed and subsequently submitted to them so informed decisions can be made.[47] Thirdly, it can

---

[42] Jackson, "Considering the Creation of a Domestic Intelligence Agency in the United States," 34.

[43] Ibid., p34–35.

[44] Ibid., 35.

[45] Loch K. Johnson, *Handbook of Intelligence Studies* (New York: Routledge, 2007), 1.

[46] Ibid.

[47] Stephen Marrin, "Intelligence Analysis and Decision-Making," in Peter Gill, Stephen Marrin and Mark Phytian, *Intelligence Theory: Key Questions and Debates* (New York: Routledge, 2009), 131.

denote a set of missions executed by secret intelligence agencies, including the collection and analysis of information, counterintelligence, counterterrorism, and covert actions. Lastly, it can refer to a set of agencies that form part of a larger community responsible for these missions. Despite differences in emphasis, all require that the raw information that has been collected be processed, and then analyzed, before it is disseminated to the policy makers.

1. Collection

Collection[48] is the gathering of raw information that will be analyzed to produce intelligence to enable policy makers to make informed decisions.[49] There are various methods and techniques that are used to fulfill this mission: imagery intelligence, signals intelligence, measurement and signature intelligence, open-source intelligence, and human intelligence.[50]

a. Imagery Intelligence

The technical developments in aviation that took place in the early 19th century significantly improved the ability of nations to observe foreign activities from an overhead vantage point. Reconnaissance aircraft were used extensively in both World War I and II to spy on opponents' fortifications and troop deployments. During the Cold War, camera-carrying satellites were initially used by the United States and the Soviet Union to monitor each other's military capabilities using techniques based on the principles of reflection of visible light, reflection of infrared radiation (heat), and reflection of bouncing radio waves to capture the image of the target. However, the most critical issue at that time was the delay between the collection and the processing phase, as they had to wait for a satellite, or part of a satellite, to return to earth in order to access the data recorded on photographic films. Nowadays, this issue is resolved. The

48 "Collection is the bedrock of intelligence, that without it the entire enterprise has little meaning." Lowenthal, *Intelligence: From Secrets to Policy*, 61.

49 Jeffrey T. Richelson, *The U.S. Intelligence Community* (Westview Press, 2012), 4.

50 Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies* (Oxford: University Press, 2008), 52.

differences in visible light levels that are reflected from targets and collected by imagery satellites are converted into digital modes and transmitted by relay satellites to ground stations almost simultaneously.

It is important to note that the number of nations with this technical capability has increased, and significant improvement has been observed in terms of the quality of images collected. Also of significance is the use of pilotless aircraft operated remotely from ground bases. The use of unmanned aerial vehicles that combine characteristics of satellites and aircraft is an important trend in recent decades, especially in combat zones such as Afghanistan and Iraq. In addition to their electro-optical, infrared, or radar-imaging sensors for imagery collection, such platforms can engage the enemy using mounted weapon systems.[51]

b. Signals Intelligence

According to Johnson, signals intelligence can be divided into two basic subcategories, communications intelligence and electronics intelligence. The former refers to the interception of communications transmitted using different means (telephones, walkie-talkies, cell phones, the Internet, and computer networks) between two parties–foreign governments, organizations, or individuals. Electronic intelligence, on the other hand, is the collection of the electronic signatures left behind by modern weapons and tracking systems in order to discover their technical capabilities.

Nowadays, signals intelligence is considered one of the most important and sensitive forms of intelligence.[52] It involves the interception, study, and analysis of foreign and domestic communication signals. This intelligence collection technique is greatly improved since the first World War, when intercept of foreign communications was mostly conducted by tapping the underwater cables of foreign nations. With the proliferation of earth-based collectors–ships, planes, ground sites, and satellites–signals intelligence is more easily picked up from the air. A recent innovation in this field is the

---

[51] Jeffrey T. Richelson, "The Technical Collection of Intelligence," in Loch K. Johnson, *Handbook of Intelligence Studies* (New York: Routledge, 2007), 105–108.

[52] "The ability to intercept communications is highly important, because it gives insight into what is being said, planned, and considered." Lowenthal, *Intelligence: From Secrets to Policy*, 91.

use of unmanned aerial vehicles as a device for the collection of signals, in addition to their image gathering capabilities, especially when tracking fast-moving targets is required, as is normally the case with terrorist activities.[53]

c. Measurement and Signature Intelligence

Measurement and Signature Intelligence[54] is technically derived intelligence data that goes beyond the technical capabilities of imagery and signals intelligence. The concept is based on the principle that certain physical characteristics of objects and events generate significant and characteristic signatures that can help in their identification and location.[55] It utilizes a wide array of collection and analysis tools, including radar, geophysical sensors, infrared and optical sensors, and nuclear radiation sensors. Ground-based and sea-based radars can detect and track missiles when they are launched, and they also have the technical capabilities to expose the characteristics of these weapons. Acoustic, seismic, and magnetic sensors can detect activities, such as nuclear tests, with geophysical properties that generate waves of a characteristic magnitude; they can also identify engines, such as submarines, with characteristic rotation speeds. Infrared and optical sensors can detect the infrared signature of missiles, aircraft, spacecraft, large detonations, and certain industrial processes. And nuclear radiation sensors can detect the x-rays and gamma rays emitted by a nuclear explosion to estimate the location of the explosion and the amount of nuclear material used.

---

53 Lowenthal, Intelligence: From Secrets to Policy, 90–91.

54 "Measurement and signature intelligence is intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydro magnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same." Department of the Army Field Manual No 2, *Intelligence* (Washington, 2010), 10–1.

55 Ibid., 10–1.

d. Open-Source Intelligence

Open source intelligence[56] refers to the study and analysis of any verbal, written, or electronically transmitted material that can be legally obtained. A former senior intelligence official argues that around 95 percent of necessary intelligence today can be obtained from these sources.[57] In fact, the development of the Internet and the changes in fields like telecommunications and science technology have expanded the arenas in which open source intelligence can be found. This wider range of open sources can be classified under six main categories: (1) Media, which includes printed documents such as newspapers and magazines as well as the news broadcast on radio and television; (2) Internet-specific sources refers to free exchange of information in forum discussions and blogs; (3) Public data consists of all reference materials available for public use, such as telephone directories, government reports, hearings and speeches; (4) Professional and academic publications can take the form of dissertations, theses, and academic papers; (5) Commercial data is exemplified by commercial imagery, and financial and industrial assessments; (6) Gray literature, which is local and foreign open source material that can only be accessed through specialized channels of distribution, like working documents, unpublished works, technical reports, and patents.[58]

e. Human Intelligence

Human intelligence is the collection of sensitive foreign information from individuals[59] who have first or second hand access to information on issues with significant implications for the security or strategic interests of the state. It can be conducted in a number of ways. The clandestine service officers may identify and then

---

56 "Open source intelligence is unclassified information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to address a specific question." Robert David Steel, "Open Source Intelligence," in Loch K. Johnson, *Handbook of Intelligence Studies* (New York: Routledge, 2007), 129.

57 Richelson, *The U.S. Intelligence Community*, 322.

58 Ibid., 321–322.

59 "Categories of HUMINT sources include but are not limited to detainees, enemy prisoners of war (EPWs), refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and non-governmental organizations." Department of the Army Field Manual No 2, *Intelligence*, 7–1.

recruit as spies individuals with access to information of value to the recruiting country. The officers responsible for collecting relevant information may operate in foreign countries under official or non-official cover. In the former case, an official job and cover makes it easier for them to maintain contact with their parent agencies. Undercover officers, on the other hand, tend to hold jobs (for example, as journalists) that allow them to move freely and ask questions without arousing suspicions. Human intelligence can be undertaken by diplomats who by virtue of their positions frequently interact both informally and formally with senior foreign government officials. Intelligence can also emanate from locals–walk-ins–who for a variety of reasons want to share information with a foreign government. Sharing intelligence by establishing a foreign liaison relationship with friendly services can be a valuable asset, especially given the fact that local intelligence agencies have a better understanding of their region.[60]

2. Processing and Exploitation

In general, most raw information collected by human or technical means does not arrive in ready-to-use form.[61] It may be necessary to process and exploit information from technical sources to convert it into a form that an analyst can use to produce finished intelligence.[62] Images must be extracted from complex digital signals and interpreted through highly refined photographic and electronic processes,[63] messages must be decrypted and foreign language intercepts translated in order to be useful.

3. Analysis

Raw information does not come with any indication of its importance or inherent meaning. It also does not provide direct clues about its relative impact on the future[64] and

---

60 Lowenthal, *Intelligence: From Secrets to Policy*, 97–103.

61 Ibid., 60.

62 Richelson, *The U.S. Intelligence Community*, 4.

63 John Hollister Hedley, "Analysis for Strategic Intelligence," in Loch K. Johnson, *Handbook of Intelligence Studies* (New York: Routledge, 2007), 213.

64 Johnson and Wirtz, *Intelligence and National Security: The Secret World of Spies*, 116.

therefore, as Bruneau argues, it is not useful without the proper analysis.[65] There is a need to put information into historical context or the context of current events, or to place it in the most appropriate analytical framework for a thorough understanding so policy and decision makers can make correct and timely decisions,[66] and also consider alternative options and outcomes.[67] In a nutshell, it can be argued that analysis[68] is the most difficult and unforgiving task in the intelligence cycle, not only because the failure to identify a potential threat is viewed as a sign of ineffectiveness, but also because it reduces the intelligence community's credibility with policymakers. Making sense of information that is often ambiguous, inconsistent, incomplete,[69] and sometimes contradictory is not an easy task.[70] Analysts are expected to assess data–identify patterns and figure out their meanings[71]—with a high level of objectivity, and must make judgments in the absence of conclusive evidence.[72]

Intelligence analysis is a perpetual fight with uncertainty in which analysts must use their own judgment and expertise on the subject matter to make sense of inherently ambiguous information in order to produce intelligence with the following characteristics.[73] Firstly, it must be passed on to the policy maker with the shortest possible delay, without waiting for a comprehensive and properly formatted document to be produced. Secondly, it should be tailored to the needs of the policymaker and omit

---

65 Bruneau and Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," in Thomas C. Bruneau, and Steven C. Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* 8.

66 Johnson and Wirtz, *Intelligence and National Security: The Secret World of Spies*, 116.

67 Hedley, "Analysis for Strategic Intelligence," 212.

68 "It includes the integration, evaluation, and analysis of all available data and the preparation of various intelligence reports." Richelson, *The U.S. Intelligence Community*, 4.

69 "[R]arely is one source from a single one of the collection categories sufficient. Sources need to be supplemented and completed to be as complete as possible and to be verified to the greatest extent possible." Hedley, "Analysis for Strategic Intelligence," 122.

70 Richelson, *The U.S. Intelligence Community*, 4.

71 "The linkage between the pattern and the meaning should come from hypotheses drawn or derived from relevant academic theory such as economics, political science, or psychology." Stephen Marrin, "Adding Value to the Intelligence Product," in Loch K. Johnson, *Handbook of Intelligence Studies*, 201.

72 William F. Brie, "Getting Intelligence Right: The Power of Logical Procedure," in *Learning with Professionals* (Washington, DC: Joint Military Intelligence College, 2005), 55.

73 Hedley, "Analysis for Strategic Intelligence," 214–215.

superfluous material. Thirdly, because policy makers do not have the luxury of time, intelligence reports should be in a format that conveys what they need to know as easily and clearly as possible.[74] Lastly, intelligence should clearly indicate what are facts, what has been added by the analysts based on their expertise, and to what extent the analysts are confident with their analysis.[75]

4. Dissemination

Dissemination, as defined by Lowenthal, is the process of conveying finished intelligence[76] to the policymakers whose needs triggered the process. It can take the form of current intelligence or long-term intelligence. Current intelligence refers to intelligence on issues that relate to day-to-day events and are the policymakers' primary concern at that point in time.[77] Long-term intelligence is more oriented towards trends and issues that are not of immediate concern, but are sufficiently important and may eventually make the headlines, especially if it does not get some current attention.[78] The dissemination of intelligence to the policymakers can be in the form of briefings and estimates, basic intelligence, warning intelligence, intelligence for operational support, and scientific and technical intelligence.

a. Briefings

Briefings are one of the most common ways of presenting current intelligence to policy makers. This direct interaction provides the opportunity for the analyst to gauge policy makers' preferences and, in the absence of a proper feedback mechanism, to evaluate the extent to which their product is seen as valuable.[79]

---

74 "They must provide added value to policy makers who probably already have a good sense of what is going on in their area of concern and a good feel for the significance and consequences of events that take place." Ibid., 212.

75 Lowenthal, *Intelligence: From Secrets to Policy*, 111.

76 "Finished intelligence refers to any intelligence product – whether a one paragraph bulletin or a lengthy study – which has completed the rigorous, all-source correlation, integration, evaluation, and assessment that enables it to be disseminated." Hedley, "Analysis for Strategic Intelligence," 212.

77 Lowenthal, *Intelligence: From Secrets to Policy*, 61.

78 Ibid., 111.

79 Ibid., 114.

b. Estimates

Estimates are judgments about the likely course of events and their impact on the state.[80] An estimate serves two important functions.[81] First, it indication of where a major issue or trend will be in the future through a projection in time which can be a period of several years. Second and more importantly, it is a combined product that presents the views of multiple agencies in the intelligence community.

c. Basic Intelligence

This refers to data–biographic, geographic, military, economic, demographic, social, and political–that have been compiled and presented in the form of monographs, in-depth studies, atlases, maps, and order-of-battle summaries.[82]

d. Warning Intelligence

Primarily a responsibility of military intelligence, warning intelligence is giving advance warning to policy makers about events that might require a policy response that would require involvement by the armed forces.[83]

e. Intelligence for Operational Support

This pertains to intelligence to support the planning and conduct of a specific operation.[84]

f. Scientific and Technical Intelligence

This refers to the assessment of developments by foreign nations or groups in the field of technology and the capabilities and performance of their weapon systems.[85]

---

80 "Estimate intelligence takes stock of what is known, and then delves into the unknown, even the unknowable." Hedley, "Analysis for Strategic Intelligence," 214.

81 Lowenthal, *Intelligence: From Secrets to Policy*, 111.

82 Hedley, "Analysis for Strategic Intelligence," 214.

83 Lowenthal, *Intelligence: From Secrets to Policy*, 114.

84 Hedley, "Analysis for Strategic Intelligence," 214.

85 Ibid., 214.

C. OPERATING WITHIN A DEMOCRATIC FRAMEWORK

The 2008 terrorist attack in India is a bitter and harsh reminder of the increasing severity of terrorist acts in recent decades. States where serious acts of terrorism have been staged find it very difficult to battle an invisible enemy who uses an asymmetrical *modus operandi*. Consequently, and for a number of practical reasons, this emerging threat calls into question the efficiency and effectiveness of the conventional means traditionally used by intelligence agencies.[86] Terrorist cells are very difficult to locate by conventional technical collection systems that use satellites, as they present a smaller imagery target.[87] Their signals communications are harder to intercept with signals intelligence sensors, not only because they offer much smaller signatures, but more specifically because some terrorist organizations have developed strategies to evade interception.[88] The collection of intelligence on terrorist cells using human resources is not an easy task. It is difficult to penetrate radical groups because potential members are carefully scrutinized and membership restricted to certain categories of individuals, based on specific criteria such as race, ethnicity and religious affiliation.[89] However, this does not imply that intelligence agencies should resort to practices that undermine the democratic principles that they are expected to uphold. There is a need for a legal framework and executive, legislative, judicial, and internal mechanisms to ensure that security intelligence agencies operate within a democratic framework and are accountable to the civil society.

1. Legal Framework

Legal recognition is one thing, but most importantly, the legal charter must define the role and responsibilities of the agencies–what they can and cannot do–along with mechanisms for overseeing their work, procedures for designating the agency head, duties of the officer in charge and his reporting channel, the staffing and recruitment

86 Thomas C. Bruneau, "Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism," *International Journal of Intelligence and Counterintelligence* 21, no. 3 (2008), 456.

87 Lowenthal, *Intelligence: From Secrets to Policy*, 84.

88 Ibid., 93.

89 Ibid., 102.

process, budget allocation, provisions making agency officials liable to judicial prosecution in case of abuses, and procedures for civil society access to government information.[90] Security intelligence agencies acquire a legal status and legitimacy when they are established and granted statutory powers under legal provisions. For example, in the United Kingdom the 1989 Security Service Act legally recognized the existence of MI5, while the Intelligence Service Act of 1994 granted legal status to MI6 and GCHQ.[91]

In the United States, intelligence agencies do not operate in isolation, but are part of an intelligence community[92] established by the National Security Act of 1947. The Intelligence Reform and Terrorism Prevention Act of 2004 defines the members of the U.S. intelligence community and outlines their role and responsibilities. These roles, all designed to protect U.S. security interests, are to collect and analyze information related to international terrorism, drug trafficking, hostile activities by foreign powers, organizations, persons and their agents, along with activities by foreign intelligence services.[93] Laws also govern the use of wiretaps by intelligence agencies for the collection of foreign intelligence, the Foreign Intelligence Surveillance Act (FISA),[94] and the right of access to government information under certain conditions granted by the Freedom of Information Act.[95]

---

[90] Thomas C. Bruneau and Florina C. Matei, "Intelligence in the Developing Democracies: The Quest for Transparency and Effectiveness," 764.

[91] Ian Leigh, "Intelligence and the Law in the United Kingdom," in Lock K. Johnson, *National Security Intelligence* (Oxford University Press, 2010), 639–640.

[92] "[The intelligence community] is made up of agencies and offices whose work is often related and sometimes combined, but they serve different clients and work under various lines of authority and control." Lowenthal, *Intelligence: From Secrets to Policy*, 10.

[93] The seventeen agencies and organizations comprising the U.S. intelligence community are listed on the Office of the Director of National Intelligence website at http:www.intelligence.org/about-the-intelligence-community/ (accessed August 30, 2011).

[94] Elizabeth R. Parker and Bryan Pate, "Rethinking Judicial Oversight of Intelligence," in Thomas C. Bruneau and Steven C. Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), 62.

[95] Ibid., 52.

2. Executive Control

Matei argues that defining the legal parameters for security intelligence agencies' operations is not sufficient to control their behavior and make them accountable for their actions.[96] Consequently, they require effective control from the executive branch, with whom they work most closely, to set their priorities and monitor how they execute their tasks. For example, in the U.S., the President's Foreign Intelligence Advisory Board is responsible for reviewing the performance of all intelligence agencies, the Intelligence Oversight Board reviews oversight by inspectors general and the general counsels of the various intelligence agencies, and the Office of Management and Budget reviews intelligence budgets in line with policies and priorities.[97] In contrast, in the U.K., the ministerial responsibility for the Security Service is under the Home Secretary, who is directly responsible to Parliament for all activities undertaken by MI5. The Service has to request authorization from the minister for actions where civil liberties and human rights are at issue.[98] It is important to note that the Director General of MI5 is "named in law as having day-to-day responsibility" and there are specific provisions in law to ensure that the agency remains politically neutral. Furthermore, the Security Service is required to submit an annual report to the prime minister and the secretary of state.[99]

3. Legislative Control

Given that the executive is the most important client of the intelligence community, there is a need to balance the power of the executive branch with a legislative control.[100] In the U.S., Congressional oversight was implemented in the

---

96 Florina Cristiana Matei, "Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy," *International Journal of Intelligence and Counterintelligence*, Vol. 20, (2007), 635.

97 Steven C. Boraz, "Executive Privilege: Intelligence Oversight in the United States," in Thomas C. Bruneau, and Steven C. Boraz, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), 30.

98 Under the Prevention of Terrorism Act 2005 and the Immigration Act 1971, "[T]elephone tapping or mail opening (...) detention of terrorist suspects, and the deportation of foreign nationals on grounds of national security."

99 Leigh, "Intelligence and the Law in the United Kingdom," 644.

100 Bruneau and Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," 15.

aftermath of the Watergate scandal in the 1970's. The Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) have a Congressional mandate to oversee the work of the intelligence community and to allocate resources.[101] Legislative control is required over resources allocated to intelligence agencies for proper accountability of public funds, but also to ensure that the agencies operate to further the national interest and comply with the rule of law.[102]

In the U.K., legislative oversight is more recent, with the Intelligence Services Act 1994 establishing the Intelligence and Security Committee to oversee and manage the security and intelligence services by auditing their expenses and reviewing their policies.[103]

4. Judicial Control

A control mechanism that can investigate complaints is required to ensure that he security intelligence agencies do not violate citizens' civil rights and liberties by abusing their special powers with intrusive or covert surveillance and searches.[104] Indeed, there is a need to appraise the work of the intelligence agencies against the legal framework.[105] In the U.K., the Regulation of Investigatory Powers Act 2000 assigns judicial commissioners the responsibility of investigating the ministers' issue and authorization of warrants allowing the security and intelligence services to intercept mail and telecommunications operations. And the Investigatory Powers Tribunal has the competency to investigate public complaints against the intelligence services for alleged violations of civil rights.[106]

In the U.S. system of government, the main function of the judiciary is to safeguard the rights of individuals enshrined in the Constitution against abuses from the

---

101 Lowenthal, *Intelligence: From Secrets to Policy*, p205–212.

102 Bruneau and Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," 15.

103 Leigh, "Intelligence and the Law in the United Kingdom," 645.

104 Matei, "Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy," 639.

105 Bruneau and Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," 15.

106 Leigh, "Intelligence and the Law in the United Kingdom," 648.

executive and the legislative branches.[107] In a number of cases, the Supreme Court has used its constitutional authority to defend the civil rights and liberties of individuals in matters of national security, in particular in *Hamdi v Rumsfeld* and in *Rasul v Bush*.[108] To ensure that defendants have a right to a fair trial, the courts now allow classified evidence to be adduced in compliance with the procedures set down in the Classified Information Procedures Act.[109]

5. Internal Control

Some democratic states created apparatus within their intelligence community to enhance the oversight mechanism. In the U.S., this includes the appointment of inspectors general and general counsels to oversee certain security intelligence activities, the use of competitive analysis to generate alternative interpretations, and training facilities to enhance the professionalism of the staff. Also, policy makers created multiple agencies within the intelligence community to prevent the intelligence function from being monopolized by a single agency or individual.[110]

D. CONCLUSION

This chapter has looked at the role and responsibilities of intelligence agencies from a very broad perspective. Its main purpose is to identify their main characteristics, the different activities that must be carried out in each of the four stages of the intelligence process, as well as the legal framework and control mechanisms that must be implemented to ensure that they operate within the rule of law. To develop the CTU of the Republic of Mauritius, the lessons learned would be combined with other factors to be identified in forthcoming chapters.

---

[107] Parker and Pate, "Rethinking Judicial Oversight of Intelligence," 65–68.

[108] Parker and Pate, "Rethinking Judicial Oversight of Intelligence," 66–67.

[109] Ibid., 52.

[110] Bruneau and Boraz, "Intelligence Reform: Balancing Democracy and Effectiveness," 16.

III. THE UNITED STATES INTELLIGENCE COMMUNITY

In the United States, the intelligence agencies do not operate in isolation, but are part of an intelligence community[111] established by the National Security Act of 1947. This community is responsible for the collection and analysis of information related to international terrorism, drug trafficking, hostile activities conducted by foreign powers, organizations, persons and their agents, as well as activities undertaken by foreign intelligence services, in order to protect the U.S. security interests.[112]

Since 2004, there has been a reorganization of the U.S. intelligence community, arguably as a result of three major issues.[113] First, reorganization was a response to the terrorist attacks of September 2001. Second, it was the result of the implementation of a number of recommendations of the 9/11 Commission Report. Lastly, it was a consequence of the apparently erroneous intelligence on the existence of weapons of mass destruction in Iraq. With the implementation of the Intelligence Reform and Terrorism Prevention Act of 2004, the U.S. intelligence community can be divided into three main categories of intelligence agencies, under the central coordination of the Director of National Intelligence: military intelligence agencies, departmental intelligence agencies other than the Department of Defense, and one independent intelligence agency.

This chapter is devoted to a succinct description of the office of the Director of National Intelligence, the three main categories of intelligence agencies, and the various functional mission support units that they control. The focus is on those agencies most relevant to this study, although other agencies are discussed in order to provide adequate

111 "[The intelligence community] is made up of agencies and offices whose work is often related and sometimes combined, but they serve different clients and work under various lines of authority and control." Lowenthal, *Intelligence: From Secrets to Policy*, 10.

112 The seventeen agencies and organizations forming part of the U.S. intelligence community are available on the Office of the Director of National Intelligence website at: http:www.intelligence.org/about-the-intelligence-community/ (accessed July 7, 2011).

113 Lowenthal, *Intelligence: From Secrets to Policy*, 27.

background information about the U.S. intelligence community. Ultimately, the aim of this chapter is to identify organizations that could serve as models for the Counter Terrorism Unit of the Republic of Mauritius.

A. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

The post of Director of National Intelligence (DNI) was created in response to recommendations from the National Commission on Terrorist Attacks upon the United States. The purpose of the post is to promote intelligence sharing between the agencies of the U.S. intelligence community. The DNI is now the head of this community and the principal advisor to the President and the National Security Council (NSC) on intelligence related to national security.[114] In a nutshell, the director oversees all U.S. intelligence agencies, supervises the collection and dissemination of intelligence across the intelligence community, and is responsible for protecting intelligence sources and methods.[115] The office of the DNI includes a headquarters staff as well as the National Counterterrorism Center (NCTC), the National Intelligence Council (NIC), the National Counterproliferation Center (NCPC), and the National Counterintelligence Executive (NCIX).

1. The National Counterterrorism Center

The NCTC is responsible for analyzing all intelligence matters related to terrorism and counterterrorism, except those that relate to purely domestic terrorism, and acts as the principal adviser to the DNI on these issues. Although the DNI has the overall responsibility for the NCTC, the director of the NCTC has another major responsibility, the strategic planning of counterterrorism operations. In this role he is authorized to report directly to the President of the United Sates.[116]

---

[114] An overview of the United States Intelligence Community for the 111th Congress, 2009, on the National Criminal Intelligence Resource Center of the Bureau of Justice Assistance of the U.S. Department of Justice website at www.ncirc.gov/searchv.cfm (accessed July 16, 2011), 1.

[115] Lowenthal, *Intelligence: From Secrets to Policy*, 29.

[116] Ibid., 38–42.

2. The National Intelligence Council

The NIC is composed of National Intelligence Officers (NIOs), who are senior officials responsible for overseeing and coordinating intelligence work across the intelligence community in their assigned specialty areas. The main roles of the NIC are to conduct mid-term and long-term strategic analysis for the DNI and to produce National Intelligence Estimates (NIEs) on issues of serious concern to the intelligence community in general.[117]

3. The National Counterproliferation Center

The NCPC is responsible for the coordination of intelligence activities on the proliferation of weapons of mass destruction and related delivery systems.[118] It is a smaller organization than the NCTC, without the operational planning responsibilities of the terrorism center. It generally does not produce its own intelligence products, but rather serves as a coordination mechanism for the rest of the intelligence community's work on WMD issues.

4. The National Counterintelligence Executive

The focus of the NCIX, as its name suggests, is counterintelligence.[119] This organization employs counterintelligence specialists from a large number of agencies throughout the national intelligence and security communities to exploit and counter intelligence activities directed against U.S. interests.[120]

B. MILITARY INTELLIGENCE AGENCIES

The military intelligence agencies fall under the command of the Department of Defense (DoD), with the main mission of supporting military operations at both the regional and tactical command level by providing indications and warnings of

---

117 An overview of the United States Intelligence Community for the 111th Congress, 3.

118 Lowenthal, *Intelligence: From Secrets to Policy*, 38.

119 "Counterintelligence refers to efforts taken to protect one's own intelligence operations from penetration and disruption by hostile nations or their intelligence services." Ibid., 151.

120 An overview of the United States Intelligence Community for the 111th Congress, 2.

forthcoming attacks and the relevant intelligence support.[121] To meet these requirements, the DoD has under its direct command and control a number of agencies and units, including the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the service intelligence units.[122]

1. National Security Agency

The main missions of the NSA are to protect the U.S. National Security information systems and to collect and disseminate foreign signals intelligence. Its fields of expertise include cryptanalysis, cryptography, and foreign language analysis.[123] Although its budget and personnel totals are not publicly available, it is understood to be the largest of all the U.S. intelligence agencies.

2. Defense Intelligence Agency

The DIA is a combat support agency and a very important component of the U.S. intelligence community. Its main mission is to provide intelligence on military topics and other areas as required to support U.S. military commanders and operational forces. Much of this effort is focused overseas to help U.S. forces counter threats and challenges in combat zones.[124]

3. National Geospatial-Intelligence Agency

The NGA is responsible for the processing and exploitation of imagery intelligence and for developing map-based intelligence solutions for U.S. national defense and homeland security, and for the enhancement of navigational safety. It also

---

121 Lowenthal, *Intelligence: From Secrets to Policy*, 36.

122 Ibid., 33.

123 "About National Security Agency," on the National Security Agency website at http://www.nsa.gov/about/ mission/ index.shtml (accessed July 19, 2011).

124 "About the Defense Intelligence Agency," on the Defense Intelligence Agency website at http://www.dia.mil/about/ (accessed July 19, 2011).

assists federal agencies and first responders involved in disaster relief and homeland defense operations by providing geospatial intelligence data, products, and analyses.[125]

4. National Reconnaissance Office

The mission of the NRO is to design, build, and oversee the launch of overhead reconnaissance systems that can be used to advise the DoD on potential aggression by foreign military forces, monitor programs related to WMDs, enforce arms control treaties and assess the impact of manmade and natural disasters.[126]

5. Service Intelligence Units

The service intelligence units of the Army, Navy, Air Force, and Marine Corps are responsible for collecting and analyzing intelligence to support their respective services. These service intelligence agencies are large organizations, often employing thousands of people.

C. DEPARTMENTAL INTELLIGENCE AGENCIES

The Department of Homeland Security (DHS), the Department of Justice, the Department of State, the Department of Energy (DoE), and the Department of Treasury are the five main departments with intelligence agencies that participate in the intelligence community. The agencies within these departments are responsible for the collection of intelligence in various fields to safeguard the United States from domestic and international security threats.

1. Department of Homeland Security

Although DHS is responsible for a wide variety of homeland security functions, its founding purpose and main responsibility is to prevent and deter terrorist attacks.[127] It plays a vital role in the merging of state and local law enforcement and intelligence

---

125 "About the National Geospatial-Intelligence Agency," on the National Geospatial-Intelligence Agency website at https:www1.nga.mil/About/Pages/default.aspx (accessed July 19, 2011).

126 "About the National Reconnaissance Office," on the National Reconnaissance Office website at http://www.nro.gov/ about/nro/what.html (accessed July 19, 2011).

127 "About Counterterrorism" on the Department of Homeland Security website at http://www.dhs.gov/files/counterterrorism.shtm (accessed July 26, 2011).

information on terrorism related issues within the U.S. territory.[128] In this context, and primarily due to recommendations of the 9/11 Commission Act of 2007, the DHS has established the State, Local, and Regional Fusion Center Initiatives. This program aims to build a partnership with state and local Fusion Centers engaged in a variety of missions, including all-crimes and all-hazards as well as counterterrorism. The concept of the fusion centers is to create a platform whereby different agencies contribute resources, expertise and information to enhance their effectiveness and efficiency in responding to criminal and terrorist activity.

2. Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI), part of the Department of Justice, is primarily responsible for the enforcement of criminal laws and protecting the United States from terrorists and foreign intelligence agencies while upholding the civil liberties of American citizens. As far as terrorism is concerned, the bureau has highly specialized and technical cells, Joint Terrorism Task Forces, in 106 cities nationwide. These interagency task forces are composed of investigators, analysts, linguists, Special Weapons and Tactics (SWAT) experts, and other specialists from a large number of U.S. law enforcement and intelligence agencies.[129]

3. Bureau of Intelligence and Research

The Bureau of Intelligence and Research (INR) of the Department of State is responsible for the analysis of events and trends that could have significant effects on the foreign policy of the United States and its national security interests.[130] Although INR is one of the smaller agencies of the U.S. intelligence community, it is widely regarded as one of the most effective. It is primarily an analytical organization, with relatively few intelligence collection assets. It does receive reporting from Defense Attaches and other

---

128 "About the Intelligence Community" on the Office of the Director of National Intelligence website at http://www.intelligence.gov/about-the-intelligence-community/member-agencies/ (accessed July 26, 2011).

129 "About Protecting America from Terrorist Attack" on the FBI website at http://www.fbi.gov/about-us/investigate/ terrorism/terrorism_jttfs (accessed July 21, 2011).

130 Bureau of Intelligence and Research on the U.S. Department of State website at http://www.state.gov/s/inr/ (accessed July 21, 2011).

human resources operating in various embassies and relies also on Foreign Service officers and Civil Service specialists with in-depth in-country experience.[131]

4. Office of Intelligence

The Office of Intelligence of the Department of Energy provides technical intelligence expertise in matters related to nuclear weapons and proliferation, energy security, science and technology, and nuclear energy, safety, and waste.[132] It is also responsible for coordinating the intelligence and counterintelligence activities of the different national laboratories that operate within the United States.[133]

5. Office of Terrorism and Illicit Finance

The Office of Terrorism and Illicit Finance of the Department of Treasury is responsible for protecting the national financial system from illicit financial transactions that support terrorism, crime and narcotics.[134]

6. Office of National Security Intelligence

The Office of National Security Intelligence (ONSI) of the Drug Enforcement Administration (DEA) under the Department of Justice supports the DEA with intelligence to enforce the controlled substance laws and regulations of the United States and to assist the intelligence community in protecting national security.[135]

D. CENTRAL INTELLIGENCE AGENCY

Despite recent changes within the U.S. intelligence community, the CIA remains the single most important element of the IC, with all-source analytical capabilities that

---

131 Lowenthal, *Intelligence: From Secrets to Policy*, 37.

132 National Security on the DoE website at http://www.energy.gov/nationalsecurity/index.htm (accessed July 21, 2011).

133 Lowenthal, *Intelligence: From Secrets to Policy*, 37.

134 Terrorism and Illicit Finance on the U.S. Department of the Treasury website at http://www.treasury.gov/resource -center /terrorist-illicit-finance/Pages/default.aspx (accessed July 21, 2011).

135 An overview of the United States Intelligence Community for the 111th Congress, 13.

cover the whole world outside U.S. territorial boundaries.[136] It is responsible for the production of national security intelligence for the President, the NSC, and senior U.S. policymakers.[137] The Director of the CIA is also the National Human Intelligence Manager, responsible for managing HUMINT programs across the IC.[138] As laid out in the Intelligence Reform and Terrorism Prevention Act of 2004, the CIA Director now reports to the DNI. It is important to note, however, that the DNI does not tend to exercise operational control over the CIA, and the CIA has retained considerable autonomy.

The main operating elements of the CIA are the National Clandestine Service (NCS), the Directorate of Intelligence (DI), the Directorate of Science and Technology (DS&T), and the Directorate of Support (DS). The next section briefly describes each of these.

1. The National Clandestine Service

The NCS is responsible for the clandestine collection of foreign intelligence–primarily human intelligence–that in principle cannot be obtained by other means, and also for counterintelligence to protect U.S classified intelligence activities and institutions from penetration and disruption by foreign intelligence services and individuals.[139]

2. The Directorate of Intelligence

The DI is the agency's primary analytical arm, with expertise in areas ranging from foreign military issues to matters of foreign policy and terrorism. The DI is considered an "all source" analytic organization, assigned to analyze information

---

136 Richard A. Best Jr., "Intelligence Issues for Congress," *Congressional Research Service*, (June 2011), 3.

137 Lowenthal, *Intelligence: From Secrets to Policy*, 32.

138 "Leadership of the CIA" on the CIA website at https://www.cia.gov/about-cia/leadership/index.html (accessed July 19, 2011).

139 "About Offices of CIA" on the CIA website at https://www.cia.gov/offices-of-cia/clandestine-service/index.html (accessed July 19, 2011).

emanating from various sources and methods, including human intelligence reports, satellite photography, open source information, sophisticated sensors, and information from U.S. personnel working overseas.[140]

3. The Directorate of Science and Technology

The DS&T is the technical arm of the CIA, providing the agency with scientific and engineering capabilities to resolve critical intelligence issues.[141]

4. The Directorate of Support

The DS is responsible for the administrative and logistic support of all the agency's elements, including acquisitions, communications, facilities services, financial management, information technology, medical services, logistics, and the security of information, facilities, and technology.[142]

E. CONCLUSION

This analysis shows that the various agencies of the United States intelligence community work for different patrons and policymakers. Consequently, they are organized, equipped, and mandated to collect specific types of intelligence within their own spheres of activity. The responsibility of the DNI is to fuse together the intelligence produced from these various sources, both to compensate for the shortcomings of each agency and to benefit from their combined strength.[143] Of prime relevance to this thesis, there are a number of entities within the IC that bring together different agencies and capabilities to accomplish specific goals. The key entities for the purpose of this thesis are the National Counterterrorism Center under the Office of the Director of National Intelligence, the Joint Terrorism Task Forces led by the FBI, and the state and local Fusion Centers coordinated by the Department of Homeland Security. An in-depth

140 "About Offices of CIA" on the CIA website at https://www.cia.gov/offices-of-cia/intelligence-analysis/what-we-do.html (accessed July 19, 2011).

141 "About the Science and Technology Directorate" on the Directorate of Science and Technology website at http:www.dhs.gov/xabout/structure/editorial_0530.shtm (accessed July 19, 2011).

142 "About News and Information" on the CIA website at https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/ds-mission-driven-solutions.html (accessed July 19, 2011).

143 Lowenthal, *Intelligence: From Secrets to Policy*, 72.

analysis of these organizations focused on their organizational structures, roles, responsibilities, and procedures for inter-agency cooperation, could serve as a structural basis for efforts to organize the Counter Terrorism Unit of the Republic of Mauritius.

IV. UNITED STATES COUNTERTERRORISM MODELS

The "Final Report of the National Commission on Terrorist Attacks Upon the United States" points out that among the major flaws that allowed the 9/11 terrorist attacks to happen are the existence of fault lines within the government between foreign and domestic intelligence, and between and within the agencies of the intelligence community, especially when it comes to the managing and sharing of information.[144] In the past decade the government has adopted a strategy that rests on the centralization of resources to achieve unity of effort,[145] making countering terrorism the first priority in the U.S.[146] To identify key points that might help organize the CTU of the Republic of Mauritius, this chapter examines three counter terrorism organizations developed or reshaped by recommendations from the 9/11 Commission: the National Counter Terrorism Center, Joint Terrorism Task Forces, and Intelligence Fusion Centers.

A. THE NATIONAL COUNTER TERRORISM CENTER

The NCTC was established under the 2004 Intelligence Reform and Terrorism Prevention Act to warn of potential terrorist threats on the U.S. To fulfill that responsibility, the center is organized as a centralized body for intelligence with well-defined roles and responsibilities. It operates under the Office of the Director of National Intelligence; its director is appointed by the President with the advice and consent of the Senate.[147] Since its creation, it has brought together more than thirty different intelligence, military, law enforcement and homeland security networks. It is staffed by analysts who are fully conversant with the organizational structure, role and responsibilities of many government agencies. In a nutshell, it is basically the same concept put forward by the President in 2003 when the Terrorist Threat Integration

144 Thomas H. Kean, and Lee H. Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at http://govinfo.library.unt.edu/911/report/911Report.pdf, xvi.

145 Ibid., 399.

146 Ibid., 361.

147 Intelligence Reform and Terrorism Prevention Act 2002, Section 119 (b).

Center was established to merge and analyze all information on probable threats at a single location.[148] The NCTC created a platform for effective collection of information from government agencies and open sources. This allows improved analysis and sharing of information related to terrorism. To fulfill that responsibility, the center has access to all the intelligence agencies' databases and can also co-opt government resources to supplement its own intelligence gathering process.[149]

The primary mission of the NCTC is to integrate information from all available sources about terrorist issues and ultimately, through efficient analysis, to provide policymakers with timely and actionable intelligence to plan appropriate responses. However, it also conducts a variety of specific interrelated tasks to support the all-source analysis process. Firstly, it is responsible for maintaining a central database, the Terrorist Identities Datamart Environment, which can be shared within the intelligence community. The database includes information on known and suspected terrorists and international terrorist groups, focusing on their motivations, capabilities and the networks that support their illegal activities.[150] Secondly, daily briefings and situation reports though secure video teleconferences and regular voice and electronic contact allows the center to keep the major intelligence agencies informed round the clock on the prevailing threat level and provides the capability to track incident information. Thirdly, the center is responsible for strategic operational planning for counterterrorism efforts in liaison with all other institutions dealing with national security. Lastly, although not mandated to direct the execution of operations, the NCTC is responsible for assigning operational responsibilities to lead agencies for counterterrorism activities.[151]

---

148 Richard A. Best Jr., "The National Counterterrorism Center (NCTC): Responsibilities and Potential Congressional Concerns," *CRS Report for Congress* (January 2011), 3.

149 Ibid., 7.

150 Ibid., 6.

151 Intelligence Reform and Terrorism Prevention Act 2002, Section 119 (d).

B. THE JOINT TERRORISM TASK FORCE

The joint task force concept was first introduced in 1979 in New York City as a solution for the need for a concerted response by federal and state law enforcement to a rise in the number of bank robberies.[152] Having proved an effective model, the idea was extended to the counterterrorism program against Puerto Rican nationalists and the New Afrikaans Freedom Fighters[153] and a task force of members of the New York Police Department (NYPD) and FBI investigators was established to investigate cases related to terrorism.[154] Over the years, this joint task force was expanded to include representatives from other local and federal authorities such as the U.S. Marshals Service, the U.S. Department of State's Diplomatic Security Service, the Bureau of Alcohol, Tobacco and Firearms (ATF), the Immigration and Naturalization Service, the New York State Police, the New York/New Jersey Port Authority Police Department, and the U.S. Secret Service.[155] Subsequently, the model was replicated in other states.

Prior to September 11, 2001, there were 35 Joint Terrorism Task Forces (JTTFs) in the U.S.[156] This number increased significantly after the attacks, when the FBI implemented numerous reforms with the goal of becoming more proactive, flexible and intelligence-driven in dealing with terrorism.[157] Today there are 106 locally based JTTFs led by the Department of Justice and the FBI. They include investigators, analysts, linguists, SWAT experts, and other specialists.[158]

---

[152] Brig Barker and Steve Fowler, "The FBI Joint Terrorism Task Force Officer," *The FBI Law Enforcement Bulletin* 77, no. 11 (November 2008), 13.

[153] Joint Terrorism Task Force, (2008). In *The 9/11 Encyclopedia*. Retrieved from http://libproxy.nps.edu/form?qurl=http%3A%2F%2Fwww.credoreference.com/entry/abcne/joint_terrorism_task_force, (accessed July 21, 2011), 2.

[154] Robert A. Martin, "The Joint Terrorism Task Force," *The FBI Law Enforcement Bulletin*, 68, no. 3 (March 1999), 24.

[155] Ibid.

[156] James Casey, "Managing Joint Terrorism Task Force Resources," *The FBI Law Enforcement Bulletin*, 73, no. 11 (November 2004), 2.

[157] Jerome Bjelopera, and Mark A. Randol, "The Federal Bureau of Investigation and Terrorism Investigations," *CRS Report for Congress* (April 2011), 1.

[158] "About Protecting America from Terrorist Attack" on the FBI website at http://www.fbi.gov/about-us/investigate/ terrorism/terrorism_jttfs (accessed July 21, 2011).

The JTTF is responsible for the operational and investigative duties of the law enforcement community to prevent acts of terrorism and investigate terrorist related crimes.[159] A number of practical measures have been implemented to maximize its efficiency and effectiveness. There is a written memorandum of understanding between agencies in the JTTF.[160] The FBI is responsible for expenses like officer overtime, vehicles, gas, cell phones, and office costs that are incurred by the state and local departments in the JTTF. For proper command and control, a supervisory special agent experienced in counterterrorism investigations oversees the daily work of the task force. Each task force is basically composed of FBI special agents with expertise in domestic and international terrorism, along with federal, state, and local law enforcement officers who bring a variety of skills to a single organizational structure. The national security effort is bolstered by including police detectives with access to local criminal databases, state police or highway patrol who have statewide jurisdiction, ATF agents with specific skills and related databases, and officers of the Bureau of Immigration and Customs Enforcement with expertise in international terrorism investigations. Also, task force coordinators are appointed to manage administrative functions and to serve as the first line investigator liaison between the federal, state, and local officers serving in the JTTF. Additionally, it has been recommended that personnel should be attached to the JTTF on a fulltime basis to ensure commitment, availability, and a focus on the mission. All members, irrespective of their parent agency, are on the same footing, assigned the same work load, and encouraged to develop their own seals, patches and jackets to create cohesiveness and enhance *esprit de corps*. Because the center deals with national security information, all officers assigned to the JTTF have top secret security clearances.[161]

To summarize, the concept of bringing several agencies under a single roof to strategically analyze domestic and international terrorism threats can be beneficial to both

---

[159] Blair C. Alexander, "Strategies to Integrate America's Local Police Agencies into Domestic Counterterrorism," *U.S. Army War College Strategy Research Project*, (March 2005), 17.

[160] Blair, "Strategies to Integrate America's Local Police Agencies into Domestic Counterterrorism," 19.

[161] Casey, "Managing Joint Terrorism Task Force Resources," 2–5.

the FBI and the law enforcement agencies.[162] When multiple agencies work together, the increased dialogue and improved relationships enhance information sharing. The expertise of the seasoned FBI officers who oversee the work of the JTTF members helps them further develop their investigative techniques and broaden their knowledge of counterterrorism and national security. The JTTF members bring additional expertise based on their knowledge of local jurisdictions and street level experience from prior assignments. In addition, the parent agencies derive benefits from the partnership. During their JTTF tenure, officers gain specialized training and experience managing complex investigations. They bring these skills and knowledge home when they return to their parent units. Parent agencies also benefit by having real-time representatives who can provide information that might be useful for disrupting terrorist networks in the local community.[163] To summarize, this partnership effectively maximizes federal, state, and local law enforcement resources[164] as each agency contributes its own capabilities, experience, and equipment in a concerted effort to prevent acts of terrorism.[165]

C. INTELLIGENCE FUSION CENTERS

The establishment of Intelligence Fusion Centers is a result of the Homeland Security Advisory Council Intelligence and Information Sharing Working Group's final report. After 9/11, it was revealed that state and local law enforcement officers had encountered some of the terrorists involved in the attacks. Unfortunately, legal provisions that regulate information sharing and bureaucratic roadblocks between state and local enforcement agencies prevented disparate pieces of information from being shared. Instead they were closely kept in the databases of the individual intelligence and law enforcement agencies. As a result, the intelligence community did not connect the dots and frame the bigger picture that might have prevented these attacks. It became clear that removing barriers between state and local law enforcement agencies could improve

---

162 Ibid., 1.

163 Barker and Fowler, "The FBI Joint Terrorism Task Force Officer," 13–16.

164 Martin, "The Joint Terrorism Task Force," 27.

165 Christopher Doane, Joseph Di Renzo III, and Jeffrey Robertson, "The JTTFs: "Jointness" at Its Most Effective!" *Domestic Preparedness Journal*, (2006), 14.

information sharing, so in 2003 the Department of Homeland Security initiated the establishment of Intelligence Fusion Centers by letting homeland security grant funds be used for preventive measures to combat terrorism.[166]

Intelligence Fusion Centers[167] are central locations where local, state and federal employees work in close proximity to receive, integrate, and analyze criminal and federal intelligence as well as public and private sector data related to homeland security and counterterrorism.[168] The centers emphasize the potential for state and local enforcement and public safety agencies to make important contributions to the overall strategy of protecting domestic security. Because their work puts them in close contact with people and events, state, local and tribal law enforcement, first responders, and other private and public sector entities are far better equipped to collect information and identify emerging threats. For example, local law enforcement officials are better placed than other agencies to detect anomalies within their communities and to be the "ears and eyes" of the larger national security community. They have the option of stopping the illegal activity, or, if they take a more intelligence-led approach and work with the FBI, they can exploit it as an opportunity to extract maximum information.

Most of the 72 state and local Intelligence Fusion Centers were created by bringing together intelligence-based units with the analytical components of the states' law enforcement agencies. Most of them are located in Urban Area Security Initiative regions, which are basically large cities with high population density and numerous critical infrastructures sites. There are significant differences in their organizational

166 "Issue Brief: Establishing State Intelligence Fusion Centers," NGA Center for Best Practices, 1–3.

167 "A fusion center is defined as a collaborative effort of two or more Federal, State, local, or tribal government agencies that combines resources, expertise, and information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal and terrorist activity." "Interaction with State and Local Fusion Centers: Concept of Operations," Department of Homeland Security (December2008), 4.

168 Todd Masse, Sioban O'Neil, and John Rollins, "Fusion Centers: Issues and Options for Congress," *CRS Report for Congress,* (July 2007), 1.

structures that are tied to their specific roles and responsibilities: counterterrorism, prevention, response, recovery, or a combination of these.[169] Nonetheless, they all have some characteristics in common.

The centers all operate within a legal framework under federal regulations in addition to applicable state policies, laws and regulations.[170] To ensure that the use of private sector data, proactive approaches to criminal offences, and intelligence collection is conducted in strict compliance with privacy rights and civil liberties, officers in the Intelligence Fusion Centers are provided Technical Assistance Training by the Department of Homeland Security and the Department of Justice.[171] There is an oversight mechanism in the form of a board of governance that oversees the work of the Intelligence Fusion Centers to ensure that they operate within their legal parameters.[172] Though initially created with a primary focus on counterterrorism, today a large number of Intelligence Fusion Centers are adopting an all-crime approach because of the nexus between terrorism and some traditional crimes. Some criminal activities such as drug trafficking, money laundering, bank robbery and illegal weapons trafficking have been and are still used to finance terrorist operations. Though most Intelligence Fusion Centers perform both prevention and response functions, the greater focus is on preventing and mitigating threats before they materialize. Most centers are involved in the analytical processing of information and threat assessments to support operations and investigations. The few that are under the jurisdiction of a single state police or bureau of investigation and staffed predominantly by sworn law enforcement officials have more operational capabilities.[173] To enhance the sharing of information, the DHS has set up a network to connect the Homeland Security Data Network and the state and local agencies.[174]

---

169 Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 21.

170 Ibid., 13.

171 Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 12.

172 Ibid., 12.

173 Ibid., 23.

174 Ibid., 27.

Besides the integration of state and local law enforcement and public safety agencies into a single structure, Intelligence Fusion Centers have also established joint partnerships with federal agencies such as Joint Terrorism Task Forces and the FBI's Field Intelligence Groups. This collaboration gives them access to the FBI information system and other facilities where classified information is stored, used, discussed or processed.[175] Intelligence Fusion Center personnel are issued different levels of security clearances depending on the tasks they perform and their need for access to classified information.[176]

In short, it appears that information sharing between local, state, and federal agencies is greatly enhanced by the Intelligence Fusion Centers, and the fusion process of turning information and intelligence into actionable knowledge is helping to mitigate the threat from terrorism, with state, local, and national benefits.

D. KEY POINTS

An analysis of the three counterterrorism organizations shows that a number of issues, including staffing, interagency cooperation, secrecy, mission, and legal framework, are fundamental for a unit to consider in its efforts to professionalize its service and improve its effectiveness.

1. Human Resources

The collection of raw information and its conversion into finished intelligence is a complex process. It involves mastering various types of methods and techniques for the collection of primary data, processing this information to convert it into the format required for analysis, separating pertinent facts from the flood of information, and applying good judgment and insights to uncover meaning and significance so policy makers can craft the appropriate response. All these steps directly or indirectly require the use of human resources. Accordingly, intelligence agencies must have highly qualified staff with the appropriate expertise. They must be employed on a full time basis to ensure

175 Ibid., 28.

176 Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress," 26–27.

their commitment, availability, and focus on the mission. It is advisable to recruit from other government agencies, as experience and knowledge of how other agencies operate is an important asset. At agency level, it is important to have a mix of agents with expertise in both domestic and international terrorism. Also, all agents must follow a standard training curriculum to improve their technical expertise and to facilitate interaction among staff within and between agencies. Finally, an environment that promotes team spirit will help everyone work toward a unified organizational goal.

2. Interagency Cooperation

Interagency coordination and cooperation within the intelligence community in the fight against terrorism is a prerequisite for effective, efficient, and timely response. This can be achieved in a number of ways. There is a need at organizational level for mechanism to coordinate with liaison officers from other intelligence agencies for effective information sharing. The implementation of a standard operating procedure across agencies can create a platform for local agency participation and encourage operational best practices. The use of a common operating system for intelligence management can facilitate access to all available databases from the various intelligence agencies. A memorandum of understanding to regulate the exchange of law enforcement and intelligence information between the different agencies provides a necessary safeguard so the dissemination of intelligence does not infringe on privacy and civil liberties. Also, there is a need for standardization of classification designations and dissemination guidelines to avoid over-classification of intelligence, an obstacle to information sharing. Lastly, a feedback mechanism on the information provided is a prerequisite to make future cooperation more effective.

3. Secrecy of Intelligence

Intelligence is all about secrecy. It encompasses the secrecy of information that one holds and wants to keep secret, as well as the secrecy of the means that one uses to find out what others are keeping secret.[177] Data obtained through cooperation with the

[177] Lowenthal, *Intelligence: From Secrets to Policy*, 1.

private sector must be protected from industrial espionage that would expose weaknesses to competitors, while information gathered from the public sector must not infringe on privacy and civil liberties. For a repository of intelligence pertaining to national security, there is first a need to acquire the necessary equipment and physical infrastructure for receiving and storing classified intelligence. Secondly, a system of security clearances must be implemented to limit access to classified information to those who are entitled to receive it.

4. Proactive Measures

Despite the fact that most counterterrorism agencies do perform both prevention and response functions, the focus must be more on preventive work to detect a threat before it materializes. This can involve public awareness initiatives, like campaigns in schools, community forums and debates on terrorism and security measures. Prevention also requires a close working relationship with the security agencies responsible for protecting critical infrastructure, to assess its vulnerability to terrorist threats and advise the agencies on protective measures.

5. Legal Framework

Legal recognition is a prerequisite in a democratic society to ensure the legitimacy of its intelligence agencies. At the very onset, there is a need for a legal charter to define the role and responsibilities of the agencies and the mechanisms for oversight of their work, the selection procedures for designating the head of the agency, the duties of the officer in charge and his reporting channel, the staffing and recruitment process, budget allocation, and provisions that make officials of the agency liable to judicial prosecution in case of abuses, and that lays down the procedures for the civil society to have access to government information.[178] Secondly, intelligence agencies must operate under democratic civilian control in order to make them legitimate in the eyes of the public. Thirdly, there is need for an official acknowledgement of the existence of the various

[178] Bruneau and Matei, "Intelligence in the Developing Democracies: The Quest for Transparency and Effectiveness," 764.

agencies in the intelligence community. Lastly, the intelligence agencies must be granted statutory charters through legislative acts expressed in formal documents that specify the parameters within which they can operate.

E. CONCLUSION

This chapter has analyzed the three main U.S. counterterrorism organizations of that share some similarities with the CTU of the Republic of Mauritius. Its main purpose is to identify the key factors that are *sine qua non* for ensuring effectiveness and efficiency in combating terrorism. The concluding chapter will combine all the key issues that have been identified to best organize the CTU of the Republic of Mauritius.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ORGANIZING THE COUNTER TERRORISM UNIT OF THE REPUBLIC OF MAURITIUS: IMPLEMENTATION AND RECOMMENDATIONS

In response to the rise of terrorism in the South West Indian Ocean and its potential to threaten national stability and security, the government of the Republic of Mauritius recently established a Counter Terrorism Unit (CTU) under the supervision of the National Counter Terrorism Committee (NCTC). The mission of this unit is to collect and analyze all terrorism-related intelligence, and ultimately disseminate the finished product to the country's law and order apparatus. This agency, which is not yet fully operational, will be vital for integrating national counter terrorism efforts and strategies. Pooling all available resources and bringing multiple strands of expertise under one roof is the standard response of most democracies facing the scourge of terrorism. It will require an integrated response based on a judicious mix of the state's defense, diplomatic, intelligence and law-enforcement capabilities. However, it is important to realize that this endeavor will require significant organizational and legal changes.

This concluding chapter focuses on the implementation of the key points that have emerged in the study. The goal is to provide lessons learned and analysis to help effectively organize the CTU so it can fulfill its mission to proactively combat all forms of terrorism so as to make the Republic of Mauritius more resilient and secure. First I consider the practices that must be adopted to ensure that the unit operates within the parameters of the rule of law and without infringing on civil liberties. I then will look at the mechanisms to promote effective collection, sharing, and dissemination of intelligence among the agencies in the intelligence community. The third section is devoted to the protection of classified information against any form of leakage. I then focus on the type of structure that will enable the CTU to effectively and efficiently fulfill its mission. Lastly, I consider how the CTU can contribute to making the Republic of Mauritius more proactive in combating the threat of terrorism.

A. LEGAL FRAMEWORK

For the CTU to be legitimate under the law, there is a need at the very onset to legally recognize the Cabinet decision that established its creation in 2009. This official legal document must define the role and responsibilities of the Unit as well as the parameters within which it can operate. There must be a mechanism to ensure that the CTU operates within a democratic framework and is accountable to civil society. This section briefly describes these three requirements.

1. Legal Recognition

This can be in the form of an act of parliament that legally recognizes the existence of the CTU, much as the Intelligence Service Act 1994 granted legal status to the MI6 and GCHQ in the U.K and the Intelligence Reform and Terrorism Prevention Act of 2004 established the office of the Director of National Intelligence in the U.S.

2. Role and Responsibilities of the CTU

The role of the CTU is to collect and analyze all terrorism-related intelligence and disseminate the finished product to the country's law and order apparatus. For this purpose, I would argue that the CTU should not be involved in field investigations or field operations and consequently does not require the legal powers and authority to arrest, detain, interview, or effect searches. In fact, it would be more comparable to the intelligence agencies in the United Kingdom where there is a separation between security and policing. Security agencies in the U.K. do not have powers of arrest or prosecute and they need to work closely with the police and Crown Prosecution Service.[179] This adds another level of control and prevents abuse of authority as the police ensure that these actions are lawfully executed.

3. Accountability and Oversight

Rendering the CTU accountable for its actions can be achieved by having executive, legislative, and judicial control over the activities of the unit.

---

179 Leigh, "Intelligence and the Law in the United Kingdom," 641.

a. Executive Control

From an administrative perspective, the CTU falls under the Secretary of Home Affairs, who chairs the National Counter Terrorism Committee that oversees the work of the CTU. As this individual is directly responsible to the Prime Minister of the Republic of Mauritius, I would argue that there is a need to implement executive control at the Cabinet level to sanction his actions, especially when the authorization to conduct certain types of actions is required, such as those requiring access to privileged information. Indeed, as per the Prevention of Terrorism Act 2002, the minister responsible for national security has the authority to direct any communication service provider, including postal and telecommunications services, to retain communications data for a specified period of time.[180]

b. Legislative Control

Recognizing that policy makers will be the main customers of the CTU, there is a need to counterbalance the powers of the executive by legislative control to ensure that agency resources are used only for legitimate purposes and consistent with its mandate. This can take the form of a committee of parliamentarians responsible for overseeing the work of the CTU. This select committee must have the relevant power to perform their control function, including authority to request specific documents and the ability to liaise with the Director of the CTU or his staff to gain information about activities of the unit. This will create a bridge between secret and the political worlds and make the organization more transparent and accountable.

c. Judicial Control

For a number of reasons that will be developed later in this chapter, I foresee that the members of the CTU are likely to come from the Mauritius Police Force. Consequently, they will have a whole range of powers granted to them under the Police Act and the Prevention of Terrorism Act 2002. Under Section 9(1) (c) of the Police Act,

180 "Communication data means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose." Prevention of Terrorism Act 2002, Section 25.

any member of the Mauritius Police Force is empowered to take all lawful measures including the use of force as may be necessary for apprehending persons who have committed, or who are reasonably suspected of having committed, criminal offences.[181] For this purpose they can exercise their powers of arrest even without a warrant if they have just cause to believe that the suspect has committed or was intending to commit a crime.[182]

With regards to detention, any person arrested under reasonable suspicion of having committed an offence under Section 3, 4, 5, 6, 7, 12 or 15 of the Prevention of Terrorism Act 2002 may be detained in police custody under the instruction of a police officer not below the rank of Superintendent of Police for a period not exceeding 36 hours from his arrest, without having access to any person other than a police officer not below the rank of Inspector, or a Government Medical Officer.[183] The main purpose here is to prevent the person from alerting of other suspects who are not yet in police custody. The police have only the obligation to keep a video recording of the detained person during his period of detention in such manner as to constitute an accurate, continuous and uninterrupted record of the whole period of his detention, including his movements, interviews, and statements.

Consequently, there is a need for oversight of the powers of the CTU by the judicial apparatus of the country to ensure that the CTU operates within the rule of law. This can be achieved by the appointment of judicial commissioners created by appropriate legislation and vested with the powers necessary to execute their investigatory task of protecting civil liberties.

B. INTERAGENCY COOPERATION

According to the concept paper from the Home Affairs Division, the mission of the CTU is to collect and analyze terrorism-related intelligence for use by the law and order apparatus. It is obvious that the CTU is expected to be more like an analytical

---

[181] Police Act 1974, Section 13(F).

[182] District and Intermediate Courts (Criminal Jurisdiction) Act (amended) 1991, Section 25.

[183] Prevention of Terrorism Act 2002.

structure than a tactical unit with agents on the ground for collecting information or performing investigations. The two main ways for the CTU to gain access to raw information are through the Mauritius Police Force and through contacts with other agencies and departments in the public and private sectors.

1. Tapping the Resources of the Mauritius Police Force

The Mauritius Police Force, the national law enforcement agency, is under the command of the Commissioner of Police, who is directly responsible to the Prime Minister. For proper control of Mauritius's 720 square miles and 1.1 million residents, the Mauritius Police Force is organized into Branches and Police Divisions directly accountable to the Police Headquarters (PHQ).

The main Branches are the Special Mobile Force (paramilitary unit), the National Coast Guard, the Helicopter Squadron, the Criminal Investigation Department, the Anti Drug and Smuggling Unit, and the Special Supporting Unit for public order operations. There are six geographical police divisions, Northern, Metropolitan, Western, Eastern, Central, and Southern. Each police division is under the command of a divisional commander with the rank of Assistant Commissioner of Police who commands a number of police stations that depends on the size of its area of responsibility. The division commander also has as attachment a small team from specialized branches such as the Criminal Investigation Department and the Anti Drug and Smuggling Unit to assist in the investigation of crimes within their area of expertise.

Tapping into the resources of the Mauritius Police Force (MPF) is the most efficient and economic process. Because this network already exists and all occurrences are reported and monitored at the Police Headquarters level, it would be highly beneficial for the CTU to work in close partnership with this coordinating body for access to fresh information in real time.

2. Appointing Points of Contact

In addition to its partnership with the Mauritius Police Force, the CTU needs to establish a working relationship with some ministries of the government and certain

companies and agencies in the private sector. There will be a need to identify those entities that have access to firsthand information on security issues, as well as those with large databases acquired by virtue of the services that they provide. For example, the Ministry of Social Security will be a valuable asset as it has personal details of all people born in the country, like date and place of birth, and names of parents, as well as their photographs when they were issued the required national identity card. The Ministry of Tourism holds a variety of records, including lists of all those who have skipper's licenses and the names of all owners of pleasure crafts. And the Customs Department has records of all importers of chemicals as well as their suppliers.

In my view, once these entities are identified, the government can, for internal security purposes, request that each designate two officers (one primary and one alternate) to serve as Points of Contact responsible for establishing and maintaining an effective information and intelligence sharing network with the CTU. The CTU will then need to provide the Points of Contact with the relevant training so they can identify intelligence considerations which, when reported, would allow the unit to develop a strategic response and comprehensive methodology to combat terrorism. To maintain the partnership, the CTU must hold regular inter-agency meetings to discuss current issues related to the threat of terrorism.

With regards to the sharing of data, all government officials are bound by the provisions of the Official Secrets Act 1972, while all data controllers[184] are bound by the Data Protection Act 2004. Therefore, at this juncture, the CTU must establish a protocol for sharing of information to ensure that classified data is shared with only those who are authorized to have access to it.

184 "[Data controller] means a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed." Data Protection Act 2004, Section 2.

C. SECRECY OF INTELLIGENCE

The CTU will be a repository of national security intelligence as it will be storing a large amount of classified information[185] from the Mauritius Police Force and other agencies and departments. There is a need to classify this information based on its significance. Furthermore, the unit must set up a mechanism to control access to classified information. And it must acquire the equipment necessary to receive and transmit classified information and physical infrastructures for storage.

1. Classification of Information

The development and implementation of a proper information classification system is a prerequisite to ensure that classified information is not compromised.[186] This can be achieved by using a standardized system of agreed terminology to define different categories of classification. However, in the Republic of Mauritius, the system of classification used in the Mauritius Police Force differs from the one used in other government ministries. The police department has a two level classification system that differentiates between information that is Confidential and Secret. In contrast, at the governmental level there is a four level classification system with categories called Restricted, Confidential, Secret, and Top Secret.

Unfortunately, there is no public document that describes the differences between these categories except the Standing Orders of the Mauritius Police Force and the Government Security Instructions of November 2010. For security reasons and because I am bound by the Official Secrets Act of 1972, I cannot disclose the content of these two documents. Suffice to say, in simple terms, that the Top Secret label is used strictly for information that can be used by hostile elements to neutralize the objectives and functions of institutions and/or the state; Secret classification is for information that may

185 "Classified information is any information or material that is held by or for, is produced in or for, or is under control of the stats or which concerns the state and which must for the sake of national security be exempted from disclosure and must enjoy protection against compromise. Such information is classified either Restricted, Confidential, Secret or Top Secret according to the degree of damage the state may suffer as a consequence of its unauthorized disclosure." Botha, *Counterterrorism Training Manual*, 228.

186 "Compromise is the unauthorized disclosure or loss of classified information or information qualifying for classification, or exposure of sensitive operations, people, places or equipment, whether by design or through negligence." Ibid., 228.

be used by hostile elements to disrupt the objectives and functions of an institution and/or the state; the designation as Confidential applies to information that may be used by hostile elements to harm the objectives and functions of and individual and/or institution; and Restricted refers to information that may be used by hostile elements to hamper activities or create inconvenience to an institution or an individual. Because the CTU operates under the Home Affairs Division, I believe it would be most appropriate for the unit to align itself with the system in use at the governmental level. This would ensure compatibility and facilitate effective information sharing, especially because all government officials are bonded by the Official Secrets Act of 1972.

2. Controlling Access to Classified Information

Access to classified information should be restricted to personnel whose security competence[187] or duties permit or necessitate such access under the "need to know" principle. For this purpose, CTU personnel must have the security clearances that give them access only to information with the specified grade of classification needed for the execution of his or her official duties. It is important to regularly conduct electronic sweeps of the premises occupied by the CTU as well as the conference room where Secret and Top Secret discussions take place to detect and neutralize any electronic eavesdropping devices.

3. Securing Classified Information

Classified information remains in a perpetual state of high vulnerability and the chance of being compromised if necessary measures are not implemented to prevent other states, organizations, or individuals from identifying and exploiting security shortcomings. The CTU must have strict guidelines with regards to transmission and storing of classified information. It first requires a secure information and communication system with encryption facilities for all stake holders to prevent the hacking of classified information while it is electronically transmitted. Furthermore, the operators responsible

187 "Security competence refers to a person's integrity and reliability as regards classified and other confidential information, and includes factors such as his/her susceptibility to extortion (blackmailing) and bribery as well as negligence with regard to such information." Botha, *Counterterrorism Training Manual*, 229.

for transmitting and receiving classified information should have the highest level of security clearance. Classified data must not be transmitted through unsecure communication systems. Access to cryptographic devices should be properly monitored and used only by those with the required level of security clearance. And lastly, classified documents[188] while not in use should be kept secure in a proper vault.

D. STRUCTURING THE COUNTER TERRORISM UNIT

In order to fulfill the mission with which it is entrusted, the CTU must be organized into appropriate functional modules, recruit appropriate staff with the relevant expertise, and enlist the services of liaison officers from the specialized units of the Mauritius Police Force.

1. Organizational Structure of the CTU

Due to limited resources in terms of finance and office space, the strength of the CTU will have to be kept as small as possible in the initial stages. A plausible approach to determining the ideal figure is to look at the functions that must be fulfilled by the unit under its mandate. As the CTU will collect information from the Mauritius Police Force, various ministries and public and the private sources, the initial stage will be devoted to processing and exploiting this information before it is passed on to the analysts. This will require a processing unit as well as an analysis unit. I believe that both units should have a domestic and a regional and international desk to avoid overburdening a single desk with information. A head analyst to coordinate the work of the analyst department and serve as the security adviser to the CTU decision making board will be required. The CTU will need a security and logistics manager responsible for the security of the premises and the information technology and communications network, as well as for the safe keeping of classified data. Also, the unit needs an officer to serve as overall

188 "Document means any note or writing, whether produced by hand or by printing, typewriting or any other similar process; any copy, plan, picture, sketch or photographic or other representation of any place or article; any disc, tape, card, perforated roll or other device in or on which sound or any signal has been recorded for reproduction." Botha, *Counterterrorism Training Manual*, 229.

coordinator for all the liaison officers of the Mauritius Police Force and the various Points of Contact. Lastly, it is worth considering the inclusion of a planning cell to assist the decision making board with future planning.

2. Recruitment Process

Assuming that the initial strength of the CTU must be kept to a strict minimum, it makes sense to recruit people who can perform multiple tasks for the CTU. Unfortunately, such versatile individuals are rare or non-existent locally because we do not have institutions that provide training in the fields of processing and analysis, and consequently will have to send candidates for training overseas or bring in outside expertise to conduct a local training program with outside expertise. Therefore, I would argue that we should recruit candidates who have a good academic background, such as a bachelor's degree, that makes them suitable candidates for such training. It would be most appropriate to recruit from police officers within the Mauritius Police Force who have worked in the intelligence cells of the units involved in criminal investigations. As the Mauritius Police Force is expected to be the largest contributor of intelligence to the CTU, the latter will benefit not only from their expertise and field experience, but also from their knowledge of how other intelligence agencies within the force operate. Also, the vetting process will be easier since the CTU will be able to access the records of conduct and performance of personnel who have already served in a disciplined force.[189] Although private organizations may have more academically qualified staffs, at this stage we lack the financial means to recruit from the private sector, as the salary scale in the private sector is usually higher than in the public sector. I suggest that the best option is to recruit internally and then provide the relevant training. It will be necessary to ensure that the candidates do not leave the unit prematurely if better opportunities in terms of salary and benefits are available in the private sector. Therefore, they should be expected to sign a bond with the government to work for the CTU for at least a specified period of time, and they should be given financial incentives during the time that they will be working for the CTU. This would create a win-win situation for them and the unit. They

189 Botha, "Security vetting is a systematic investigative process to determine a person's security competence," *Counterterrorism Training Manual*, 229.

will have higher qualifications that will help them earn a better salary once they leave the organization, and they will be valuable assets while working for it.

3. Enlisting Liaison Officers

In the absence of field agents, the CTU could benefit greatly by having a group of liaison officers from the various units of the Mauritius Police Force who are directly or indirectly tied to the collection of criminal and security intelligence. Among the best candidates from this perspective would be officers from the Crime Index Unit (responsible for the control and issuing of firearm licenses), Anti Drug and Smuggling Unit, Interpol, Central Criminal Investigation Department, National Security Service, Very Important Personality Security Unit, Traffic Branch (which manages the database for all public service vehicles and driving licenses), Passport and Immigration Office, Explosive Handling Unit, *Groupe d'Intervention de la Police Mauricienne* (GIPM), Crime Record Office, Crime Information Technology Unit, National Coast Guard, and Police Information and Record Office. These officers would not be posted permanently to the CTU, but rather would meet regularly to discuss security issues related to terrorism and share information from their respective fields of operations. This will be more cost effective for the CTU than hiring full-time agents, and beneficial because these officers will have concrete, timely intelligence from their agencies.

E. PROACTIVE MEASURES

Besides the mission that it has been assigned, I would argue that the CTU can play a leading role in making the Republic of Mauritius more proactive in dealing with the threat of terrorism. Among other initiatives, it can assist security agencies responsible for the protection of critical infrastructures by assessing their security measures and working with them to make them more resilient. It might also sponsor awareness campaigns, through lectures in schools and community forums, to inform the public about terrorist threats and provide guidelines on how they should respond to suspicious activities.

F. CONCLUSION

The focus of this thesis has been on how to organize the CTU of the Republic of Mauritius by using as models the three main U.S counterterrorism agencies–the National Counter Terrorism Center, the Joint Terrorism Task Force and the Intelligence Fusion Centers. The in-depth analysis of these three models has been instrumental in identifying key issues that must be considered in any effort to promote effective information sharing among intelligence agencies and to establish agencies that are effective and efficient in fulfilling their missions.

The effectiveness of intelligence agencies is greatly enhanced when they have a full-time staff of highly qualified professionals with relevant expertise and knowledge of other agencies, all dedicated to a unified organizational goal. Effective mechanisms and platforms for the sharing of information, including liaison officers, a common database system, standard operating procedures, and memoranda of understanding, all promote interagency cooperation and help intelligence agencies to initiate timely responses. The protection of classified information can only be ensured when there is a proper system in place for sharing, accessing, and safeguarding this type of information. Legitimacy of intelligence agencies in a democratic society requires that they have legal status and operate in strict compliance with the rule of law. Lastly, combating terrorism must involve a mix of both proactive and response-oriented measures.

Organizing the CTU for the Republic of Mauritius to accommodate these points will definitely require legal and organizational changes, as well as the implementation of a number of administrative procedures. The implementation process must take into consideration the local context, specifically, the existing legal framework and availability of resources. The CTU must from the start be given a legal status with properly defined roles and responsibilities and proper oversight mechanisms to ensure that the unit operates within legal parameters. It will have to build a strong partnership with the Mauritius Police Force, which has a national network for the collection of intelligence, as well as with other public and private sector agencies that by virtue of the services they provide have compiled huge databases. The CTU must develop a protocol for classifying, accessing, safeguarding and sharing classified information to ensure that essential

intelligence is not compromised. The CTU will have to adopt an organizational structure that will allow it to effectively perform the tasks required by its mission and recruit the appropriate workforce. And in addition to its primary role, the CTU must also work with the civil society to develop proactive measures in the struggle against terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

The 9/11 Encyclopedia. "Joint Terrorism Task Force" The 9/11 Encyclopedia, http://libproxy.nps.edu/form?qurl=http%3A%2F%2Fwww.credoreference.com/entry/abcne/joint_terrorism_task_force. Accessed July 21, 2011.

Alexander, Blair C. "Strategies to Integrate America's Local Police Agencies into Domestic Counterterrorism." *U.S. Army War College Strategy Research Project*, March 2005.

Barker, Brig and Steve Fowler. "The FBI Joint Terrorism Task Force Officer." *The FBI Law Enforcement Bulletin* 77, no. 11 (November 2008): 12–16.

Best, Richard, A. Jr. "Intelligence Issues for Congress." *Congressional Research Service, Report for Congress*, (June 2011).

———. "The National Counterterrorism Center (NCTC): Responsibilities and Potential Congressional Concerns." *Congressional Research Service, Report for Congress,* (January 2011).

Betts, R. K. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press, 2007.

Bjelopera, Jerome, P. and Mark A. Randol. "The Federal Bureau of Investigation and Terrorism Investigations." *Congressional Research Service, Report for Congress,* April 2011.

Boraz, Steven C. "Executive Privilege: Intelligence Oversight in the United States." In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* edited by Thomas C. Bruneau and Steven C. Boraz. Austin: University of Texas Press, 2007.

Botha, Anneli. *Counterterrorism Training Manual*. Pretoria, South Africa: Institute for Security Studies, 2009.

Brie, William F. "Getting Intelligence Right: The Power of Logical Procedure." In *Learning with Professionals.* Washington, DC: Joint Military Intelligence College, 2005.

Bruneau, Thomas C. "Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism." *International Journal of Intelligence and Counterintelligence*, 21, no. 3 (2008): 448–460.

Bruneau, Thomas C. and Steven C. Boraz. "Intelligence Reform: Balancing Democracy and Effectiveness." In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* edited by Thomas C. Bruneau, and Steven C. Boraz. Austin: University of Texas Press, 2007.

Bruneau, Thomas C. and Florina C. Matei. "Intelligence in the Developing Democracies: The Quest for Transparency and effectiveness." *International Journal of Intelligence and Counterintelligence* 20 (2007): 757–773.

Casey, James. "Managing Joint Terrorism Task Force Resources." *The FBI Law Enforcement Bulletin* 73, no. 11 (November 2004): 1–6.

Central Intelligence Agency. "About News and Information" Central Intelligence Agency, https://www.cia.gov/news-information/ featured-story-archive/2008-featured-story-archive/ds-mission-driven-solutions.html. Accessed July 19, 2011.

———. "About Offices of CIA" Central Intelligence Agency https://www.cia.gov/offices-of-cia/clandestine-service/index.html. Accessed July 19, 2011.

———. "Leadership of the CIA" Central Intelligence Agency, https://www.cia.gov/about-cia/leadership/index.html. Accessed July 19, 2011.

Cline, E. L. "Interagency Decision Making." In *Civil-Military Responses to Terrorism*, edited by the Center for Civil-Military Relations. California: Naval Postgraduate School, 2011.

Dahl, J. E. "Intelligence and Terrorism." In the *International Studies Encyclopedia*, part of the *International Studies Association Compendium Project*, edited by Denemark R. et al. Oxford: Wiley-Blackwell, 2010.

Defense Intelligence Agency. "About the Defense Intelligence Agency" Defense Intelligence Agency, http://www.dia.mil/about. Accessed July 19, 2011.

Department of Energy. "National Security" Department of Energy http://www.energy.gov/nationalsecurity/index.htm. Accessed July 21, 2011.

Department of Homeland Security. "About Counterterrorism" Department of Homeland Security, http://www.dhs.gov/files/counterterrorism.shtm. Accessed July 26, 2011.

———. "Interaction with State and Local Fusion Centers: Concept of Operations." *Department of Homeland Security*,(December2008).

Department of State. "Bureau of Intelligence and Research" U.S. Department of State, http://www.state.gov/s/inr. Accessed July 21, 2011.

Department of the Army Field Manual No 2. *Intelligence*. Washington, 2010.

Department of the Treasury. "Terrorism and Illicit Finance" Department of the Treasury, http://www.treasury.gov/resource -center /terrorist-illicit-finance/Pages/default.aspx. Accessed July 21, 2011.

Directorate of Science and Technology. "About the Science and Technology Directorate" Directorate of Science and Technology, http:www.dhs.gov/xabout/structure/editorial_0530.shtm. Accessed July 21, 2011.

Doane, C., J. Di Renzo III, and Jeffrey Robertson. "The JTTFs: "Jointness" at Its Most Effective!" *Domestic Preparedness Journal*, (2006), 14–15.

Federal Bureau of Investigation. "About Protecting America from Terrorist Attack" Federal Bureau of Investigation http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs. Accessed July 21, 2011.

Hedley, John Hollister. "Analysis for Strategic Intelligence." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson. New York: Routledge, 2007.

Hoffman, B. "Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post Cold War Era." *Intelligence and National Security* 11, no. 2 (1996): 207–223.

Intelligence Reform and Terrorism Prevention Act 2002, Section 119 (b).

Jackson, B. A. *Considering the Creation of a Domestic Intelligence Agency in the United States*. Washington, DC: RAND Corporation, 2009.

Jenkins, Brian. "Statement to the National Commission on Terrorist Attacks Upon the United States." Washington, 2003, http://govinfo.library.unt.edu/911/hearings1/witness_jenkins.htm. Accessed May 25, 2011.

Jervis, Robert. "Intelligence, Civil-Intelligence Relations, and Democracy." In *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* edited by Thomas C. Bruneau, and Steven C. Boraz. Austin: University of Texas Press, 2007.

Johnson, Loch K. *Handbook of Intelligence Studies*. New York: Routledge, 2007.

Johnson, Loch K. and James J. Wirtz. *Intelligence and National Security: The Secret World of Spies*. Oxford University Press, 2008.

Kean, T., and L. Hamilton. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at http://govinfo.library.unt.edu/911/report/911Report.pdf.

Laws of Mauritius
http://www.gov.mu/portal/site/GovtHomePagesite/menuitem.c0a01177fcf48dfcf6be501054508a0c/?content_id=8b4484d776e98010VgnVCM100000ca6a12acRCRD. Accessed Oct 29, 2011.

Leigh, Ian. "Intelligence and the Law in the United Kingdom." In *National Security Intelligence,* edited by Lock K. Johnson. Oxford University Press, 2010.

Lowenthal, M. *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press, 2006.

Marrin, Stephen. "Adding Value to the Intelligence Product." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson. New York: Routledge, 2007.

———. "Intelligence Analysis and Decision-Making." In *Intelligence Theory: Key Questions and Debates* edited by Peter Gill, Stephen Marrin, and Mark Phytian. New York: Routledge, 2009.

Martin, Robert A. "The Joint Terrorism Task Force." *The FBI Law Enforcement Bulletin*, 68, no. 3 (March 1999): 23–27.

Masse, T., S. O'Neil, and J. Rollins "Fusion Centers: Issues and Options for Congress." *CRS Report for Congress,* (July 2007).

Matei, Florina C. "Romania's Intelligence Community: From an Instrument of Dictatorship to Serving Democracy." *International Journal of Intelligence and Counterintelligence* 20 (2007): 629–660.

National Criminal Intelligence Resource Center of the Bureau of Justice Assistance of the U.S. Department of Justice. "An overview of the United States Intelligence Community for the 111th Congress, 2009" National Criminal Intelligence Resource Center of the Bureau of Justice Assistance of the U.S. Department of Justice, www.ncirc.gov/searchv.cfm. Accessed July 16, 2011.

National Geospatial-Intelligence Agency. "About the National Geospatial-Intelligence Agency" National Geospatial-Intelligence Agency, https:www1.nga.mil/About/Pages/default.aspx. Accessed July 19, 2011.

National Reconnaissance Office. "About the National Reconnaissance Office" National Reconnaissance Office, http://www.nro.gov/ about/nro/what.html. Accessed July 19, 2011.

National Security Agency. "About National Security Agency" National Security Agency, http://www.nsa.gov/about/ mission/ index.shtml. Accessed July 19, 2011.

NGA Center for Best Practices. "Issue Brief: Establishing State Intelligence Fusion Centers." *NGA Center for Best Practices.*

Office of the Director of National Intelligence. "The seventeen agencies and organizations forming part of the U.S. intelligence community" Office of the Director of National Intelligence, http:www.intelligence.org/about-the-intelligence-community. Accessed July 7, 2011.

———. "About the Intelligence Community" Office of the Director of National Intelligence, http://www.intelligence.gov/about-the-intelligence-community/member-agencies/. Accessed July 26, 2011.

Parker Elizabeth R. and Bryan Pate. "Rethinking Judicial Oversight of Intelligence." in *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness,* edited by Thomas C. Bruneau, and Steven C. Boraz. Austin: University of Texas Press, 2007.

Posner, R. *Countering Terrorism: Blurred Focus, Halting Steps*. Lanham MD: Rowman and Littlefield, 2007.

Richelson, Jeffrey T. "The Technical Collection of Intelligence." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson. New York: Routledge, 2007.

———. *The U.S. Intelligence Community*. Westview Press, 2012.

Robinson, M., and D. Last. "A Basic Model of Performance-Based Budgeting." *International Monetary Fund*, September 2009.

Sinclair, A. "Approaches to Organisational Culture and Ethics*." Journal of Business Ethics* 12, no. 1 (January 1993): 63–73.

Steel, Robert David. "Open Source Intelligence." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson. New York: Routledge, 2007.

Zegart, A. *Spying Blind: The CIA, the FBI, and the Origins of 9/11*. Princeton: Princeton University Press, 2007.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Erik Dahl
   Naval Postgraduate School
   Monterey, California

4. Professor Maria Rasmussen
   Naval Postgraduate School
   Monterey, California

5. Professor Paul Shemella
   Naval Postgraduate School
   Monterey, California

6. Captain Jennith Hoyt
   Naval Postgraduate School
   Monterey, California

7. Commander Tim Unrein
   Naval Postgraduate School
   Monterey, California

8. Mr. Randy Burkett
   Naval Postgraduate School
   Monterey, California