SELINUS UNIVERSITY
OF SCIENCES AND LITERATURE

THREATS AND THE NEED FOR DOMESTIC INTELLIGENCE REFORM

By URSOEL KUYUNGANA MAYUMBU

A DISSERTATION

Presented to the Department of
Intelligence, Global Security and Counterterrorism
Program at Selinus University

Faculty of Arts & Humanities
In fulfillment of the requirements
for the degree of Doctor of Philosophy in
Intelligence, Global Security and Counterterrorism Studies

2023

DEDICATION

I dedicate this thesis to my parents. Without their patience, understanding, support, and, most of all, love, the completion of this work would not have been possible.

ACKNOWLEDGMENTS

I would like to personally thank the members of my community and my children ***Mayumbu Bertrand, Mayumbu Methoushella, Mayumbu Candide, Mayumbu Harmony, Prisca Audrey Mayumbu Mayumbu George William, Mayumbu Levi Israel, Mayumbu Xaviera Serena, and My Partner Munginda Yene Matondo and my wife Mayumbu May Rhonda*** for their support, patience, and good humor. Their gentle but firm direction has been most appreciated. Dr. Salvatore Fava, my Thesis General Supervisor, was particularly helpful in guiding me toward a qualitative methodology and his interest in a sense of competence was the impetus for my proposal. Finally, I would like to thank my professors, of Selinus University. From the beginning, they had confidence in my abilities to not only complete a degree, but to complete it with excellence.

I have found my course work throughout the Intelligence Studies program to be stimulating and thoughtful, providing me with the tools with which to explore both past and present ideas and issues.

ABSTRACT OF THE THESIS
TERRORIST THREATS AND THE NEED FOR DOMESTIC INTELLIGENCE REFORM

by

Ursoel K. Mayumbu
Selinus University, July 2024

Dr. Salvatore Fava, Thesis General Supervisor,

Many countries worldwide do not have adequate intelligence agencies to predict and prevent terrorism. Currently, there are three significant threats at the national level: jihadist terrorism, far-right terrorism, and great power competition, which can be described as "great power incursion." The latter could potentially target the United States and its allies. Unfortunately, the current resources of the DHS and the FBI are insufficient to effectively combat these threats and ensure global security. Given these circumstances, this thesis aims to address the following research question: Given the prevalence of dynamic threats to national and global security, how should the new intelligence structure that specializes in terrorism be designed and implemented to protect the United States and its allies? This dissertation discusses the intelligence cycle, OSINT, biometrics, and the threats of terrorism posed by groups such as Al-Qaeda in Afghanistan, the Islamic State (ISIS) in Iraq and Syria, and Boko Haram in Africa. These threats highlight the need for intelligence reform to effectively respond to threats to state safety and security. This thesis aims to identify a suitable security model by examining the elements necessary for an effective policy and focusing on the characteristics of a domestic intelligence agency. It reviews theories of intelligence and evaluates their application. Lessons learned from case studies of the United States, the Democratic Republic of the Congo, and the United Kingdom show that balancing transparency and efficiency is complex yet necessary to safeguard state security. The results of this research conclude that current national intelligence agencies are not sufficiently equipped to respond to these threats and require significant reform.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF ABBREVIATIONS

CI	Counterintelligence
CONUS	Continental United States
DHS	Department of Homeland Security
DNI	Director of National Intelligence
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FISS	Federal Information Security Management Act
HUMINT	Human Intelligence
HVT	High Value Target
IC	Intelligence Community
ISIS	Islamic State of Iraq and Syria
MSPP	Multi-State Plan Program
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
OCONUS	Outside of the Continental United States
OFCO	Offensive Counterintelligence
OPM	Office of Personnel Management
OPSEC	Operational Security
OSINT	Open-Source Intelligence
PII	Personally Identifiable Information
RTP	The Rendition Project
TSCM	Technical Surveillance Countermeasures
TTPs	Tactics, Techniques, and Procedures
USG	United States Government
USIC	US Intelligence Community, Global Security

LIST OF FIGURES

FIGURE PAGE

LIST OF TABLES

TABLES PAGE

CHAPTER ONE

Overview

This dissertation aims to explore improved methods that will facilitate a broad understanding of the challenges of terrorism. It also aims to demonstrate the current weaknesses in the intelligence cycle of countries allied with the United States. Through an in-depth analysis of the key elements of the intelligence cycle, this dissertation will propose the creation of a specialized domestic counterterrorism intelligence structure that will benefit both the United States and its allied countries (Schmid, A.P., Forest, J.J.F., and Lowe, T., 2021).

There is much inefficiency in the intelligence systems of countries allied with the United States. These inadequacies prevent intelligence agencies from effectively combating terrorist groups. The main goal of intelligence systems is to identify, penetrate, manipulate, deceive, and suppress individuals, groups, or organizations suspected of espionage activities. The intelligence system has two main activities: counter-espionage, which aims to counter threats linked to foreign intelligence, and counter-terrorism, which specializes in preventing any terrorist threat. Counterterrorism is an area that has received less attention and research compared to terrorism. According to Byman and Daniel (2007), counterterrorism is "under-theorized and understudied". While there are numerous definitions of terrorism, there are far fewer definitions for counterterrorism or "anti-terrorism." This is because counterterrorism is a reactive phenomenon that does not require much explanation (Byman, Daniel, 2007).

Terrorism has grown on all continents. The overall deterioration of security makes the terrorist threat “increasingly complex and decentralized”. Extremists are currently using the most modern means and sophisticated technologies, such as drones and artificial intelligence, to plan and carry out terrorist attacks.

Given the scale and scope of the threat linked to radicalization in the context of terrorist acts and similar crimes, intelligence structures should adapt new technologies and put in place apprehension structures, known in the field of counter-terrorism intelligence as "perceived threat", to unmask influences, which are describable as major factors in the propagation and adoption of extremist ideologies, and which often contain elements of the collective complaint and subsequent acts of violence. (Hoffman, A. M., & Shelby, W., 2017; Mandel, D. R., 2003; Matthes, J., Schmuck, D., & von Sikorski, C., 2019)

Anti-terrorism operational intelligence is a new type of intelligence that is both descriptive and predictive. It helps decision-makers and leaders apprehend people suspected of having intended or having committed terrorist acts, before or after an attack. In counter-terrorism, there are three essential elements: descriptive analysis, diagnostic analysis, and predictive analytics. Descriptive analysis tells you what happened in the past, diagnostic analysis helps you understand why something happened in the past, and predictive analytics predicts what is most likely to happen in the future. Predictive intelligence is a broader concept that encompasses all forms of data-driven prediction, while predictive analytics is a specific approach that relies on modeling and statistical analysis (Aljohani, Abeer. 2023).

In counter-terrorism operations, two intelligence structures should be complementary forces but carry out different operations: descriptive and predictive. The primary explanatory factor is the perceived threat. In general, the higher or more visible the perceived threat, the more active the investigations carried out by counterterrorism officers should be.

They should investigate all possibilities of money laundering, investments in buildings, gas stations. Unfortunately, these investigations often go to the detriment of civil liberties. (Huddy et al., 2005, 2007; Haider-Markel et al., 2006)

Background of the Problem

After the devastating terrorist attacks of September 11, 2001, the fight against terrorism became a top priority for the United States government. In response, the government swiftly developed a security framework to protect the country against large-scale attacks from foreign sources. Federal, state, and local capacities were strengthened to prepare for, respond to, and recover from domestic threats and disasters. During this period, new institutions were created, including the Department of Homeland Security (DHS), the National Intelligence Directorate (DNI), and the National Counterterrorism Center (NCTC), which greatly increased resources for intelligence and law enforcement. However, the focus on protecting the United States led to the neglect of mechanisms for protecting allied countries from international gangs. This neglect resulted in dire consequences, as emphasized by Pomerantz, SL, (1987).

Precipitous consequences of excessive U.S. self-protection

The rush to prioritize self-protection over allied countries and increased counterterrorism scrutiny in the American security system has had eight major global consequences.

First, the following text talks about the negative impacts of biometric detection technology on some members of the Counterintelligence (CI) and Department of Defense (DoD), leading to problems for authorized U.S. counterintelligence personnel working overseas and using fake passports. This has prompted several allied countries to take measures at border crossings and other checkpoints around the world to identify problematic individuals through biometric processes (Kloppenburg 2013).

Second, although mass surveillance has resulted in positive outcomes for protecting the United States, it has come at a considerable strategic, material, and human cost. This has affected border personnel, who operate under alternative identities to foreigners and are forced to make compromises when passing through checkpoints in hostile countries that employ biometric identification technologies, such as India's Unique ID project (Rao and Greenleaf 2013).

Thirdly, one of the major consequences of mass surveillance would be the migration of terrorists to other favorable territories where the counter-terrorism intelligence system is weak or has not yet been established. This affects all methods of information gathering and the intelligence cycle.

Terrorist groups are operating outside of the United States, which pose a significant threat to the American homeland. Several foreign terrorist organizations, such as Al-Shabaab in East Africa and ISIS in West Africa, are active across the African continent. These groups share similar ideologies and distorted perceptions of Islam. Their ultimate goal is to establish caliphates that extend beyond the borders of the countries in which they operate. These terrorists cooperate with rival factions, armed groups, regional forces, and militias. This is what ISIS accomplished in Syria and Iraq around 2014.

Fourth, Migration led to the birth of new terrorist groups like Al-Qaeda (Afghanistan), which inspired ISIS (Iraq) and Boko Haram (Nigeria).

Fifth, the creation of conflicts and foreign policy crises around the world is one of the harmful consequences of decision-making regarding global security. These conflicts are not likely to disappear anytime soon. Many of these conflicts are caused by countries making decisions without consulting the regions concerned. Regions such as Europe, South America, the Middle East, and Africa are particularly affected by this issue.

Sixth, due to a hasty and erroneous judgment on the establishment of anti-terrorism structures by the United States, the world is today confronted with three major threats at the national level of each country: jihadist terrorism, extreme terrorism right-wing and great power competition , described as a “great power incursion” and targeting the United States and its allies. The current resources of the DHS and the FBI are no longer sufficient to effectively fight for global security against these threats.

Seventh, the restriction of sponsored group terrorism in the United States led to a new type of terrorism known as "lone wolf" terrorism. This change occurred as radicalized individuals adapted their modus operandi. Unlike traditional terrorists who operate in organized groups, lone-wolf terrorists work alone. They have become a major concern for the intelligence community as they are difficult to detect and combat. Even though terrorists have migrated to other continents, lone-wolf terrorists remain a significant threat.

The lack of consideration for the security of allied countries while establishing a new counterterrorism structure in the US system had severe repercussions. This move not only undermined the security policies of allied countries but also put at risk the democratic principles and processes they sought to preserve. As rightly pointed out by Crenshaw, M. (Ed. 2010), it is vital to take into account the interests of all involved parties to ensure a secure and democratic world order (Crenshaw, M. (Ed. 2010).

Statement of the Problem

The terrorist attacks on September 11, 2001, had a significant impact on the American intelligence system and global security. In the current era of terrorism, several countries lack predictive intelligence agencies to prevent terrorism. They face three major threats at the national level, namely jihadist terrorism, far-right terrorism, and great power competition, which could be described as "great power incursion," and may target the United States and its allies. Unfortunately, most analyses of predicting terrorism are not effective. Most forecasts seem to reflect the current state of terrorism rather than its future (Bakker, E., 2012).

The terrorist attacks that occurred on September 11, 2001, in the United States led to the widespread use of biometric systems at airports and border crossings worldwide to identify criminals and terrorists. Since then, the United States has not experienced any other significant foreign terrorist attacks, except for those carried out by individuals acting alone, also known as "lone wolves". However, the number of attacks by unaffiliated individuals and groups has increased in recent years (Worth, 2016).

The United States created new security system institutions, including the Department of Homeland Security (DHS), the National Intelligence Directorate (DNI), the National Counterterrorism Center (NCTC) and the US Intelligence Community (USIC). This gigantic security system is subdivided into several agencies that make up the protection and defense apparatus of the United States (Christopher R Moran, Joe Burton, George Christou, 2023).

Additionally, the United States has implemented new security procedures to restore air travel security. A finding has emerged in favor of the development of American military and intelligence capabilities, endowed with the power of persuasion to foil numerous plots, dismantle terrorist financing networks, and track down terrorist leaders, notably Osama bin Laden in 2011.

The U.S. military and intelligence services have stayed ahead of rapidly changing technologies. These intelligence efforts have helped improve U.S. homeland security. However, these security initiatives have generated significant financial, moral, and strategic opportunity costs and have not taken into account the overall counter-terrorism strategy.

The United States of America, a few years after the militarized response to the September 11 attacks and the analysis related to global terrorism, began to recognize the limits of a military-centric approach and the need to redefine overall security. Unfortunately, no fundamental changes have been proposed in favor of a new international approach. The incapacity of an approach centered on the army is decried by this present study which calls for the establishment of an anti-terrorist intelligence system, implying a hierarchy between diplomacy, military tools, economic tools, and international diplomacy. Efforts to integrate “counterterrorism intelligence power” as a central concept of national and international security will achieve the promised and desired results.

The United States should change its past behavior by effectively using foreign aid and other related tools to achieve its overall security objectives. According to Czwarno, peers failed to predict or warn of the possibility of the September 2001 terrorist events in the United States. This inability to predict terrorism is manifested by the absence of an anti-terrorist intelligence structure capable of helping the allies of the United States (Monica Czwarno, 2006).

The threat of terrorism is a major concern for all nations, and countries allied with the United States should have access to the best intelligence systems available. However, it has become clear that the system currently in use is not adequate to prevent or detect terrorist attacks. It's time to invest in a specialized system that will provide allies with the tools they need to stay ahead of this growing threat and keep their citizens safe. The solution could be the creation of a new counterterrorism structure in each country allied with the United States.

Evidence of the lack of appropriate instruments to combat terrorism can be seen in reference to the Department of Homeland Security (DHS) policy framework, which recognizes the existence of a line between terrorism and targeted violence but difficult to draw. (U.S. Department of Homeland Security, 2019)

A. Research Question

Intelligence plays a crucial role in helping countries anticipate and prevent the various security challenges they face regularly. Given the prevalence of dynamic threats to domestic and global security, it is important to consider how a new intelligence structure, specifically focused on counterterrorism, should be established and utilized to protect the United States and its allies.

B. Significance of the Research Question

In today's world, nations face a plethora of security challenges that can put their citizens and interests at risk. Intelligence is crucial to identify and prevent such threats. Thus, all countries should recognize the importance of intelligence and invest in it to safeguard their people and interests (Mark M. Lowenthal, 2015; Loch K. Johnson, 1983; Richard K. Betts, 2007)

The draconian measures taken by the United States to protect themselves from terrorism have produced discouraging consequences. There is a public perception, both within and near U.S. allied countries, that governments' capacity to combat terrorism, crime, and border violence is weak. This thesis will analyze the key elements for designing a national structure for the protection of allied countries.

This research carries immense significance for three critical audiences - US governments, allied countries, and security sector practitioners. By providing valuable strategic and tactical information, this study can help shape policies, promote security, and bolster defense mechanisms. Hence, this study recognizes the potential impact of this research work and utilizes its insights to strengthen national security and global stability.

Definition of Terms

Intelligence

Functional Definition: Intelligence is the product resulting from the collection, compilation, evaluation, analysis, integration, and interpretation of information gathered against an adversary to promote the national interest.

Essential definition: The term intelligence is essentially defined as the technique that covers the scientific and technical monitoring of research progress, the forecasting of future systems, the knowledge of defense systems in service, and the prevention of strategic surprises, particularly in matters of proliferation of defense systems, weapons of mass destruction, terrorism, and espionage, which were not considered science and which it was believed that everyone was naturally capable of and did not need to be studied » (Lewal, 1881).

One of the most important functions of intelligence is to reduce the ambiguity inherent in observing external activities. Intelligence has been relegated to the secrecy of political and military power, as a sub-branch while all theorists agree that intelligence is essential to strategic decision-making (Coutau-Bégarie, 1999; Franck Bulinge and Éric Boutin, 2015)

Faced with the paradigm shift represented by the end of the Cold War and the democratization of information and communication technologies, intelligence, relegated to the background, has today become an object of research in the human and social sciences, through work on monitoring and documentary information.

Terrorism: The word terrorism does not have a common definition for all countries or a legally adopted understanding. The definition of terrorism and its scope are politically complex and its selective use is often the subject of controversy within and outside domestic and international legal arenas (Finley, CJ, 2015).

The reason for the lack of a common definition can be understood in the following reflection: a terrorist is considered a freedom fighter in his country, but is considered an enemy in the Adeverse camps. What is included in the phrase "One man terrorist, another freedom fighter" (Ganor, B., 2002)

According to FBI there is no common definition acceptable to all because. Domestic or international terrorism is the unlawful use of violence against persons or property to intimidate or coerce a government or civilian population in the pursuit of political or social objectives. The FBI's specialty as an agency is primarily operational response to domestic terrorism. (Pomerantz, SL, 1987).

Lone Wolf: The term lone wolf was defined by Burton and Stewart as "a person who, under his sole direction, carries out terrorist actions, without orders or even without links to an organization (Fred Burton and Stewart, Scott, 2008; Dixon, A. L., Gassenheimer, J. B., & Barr, T. F., 2003).

The term "Lone Wolf" was based on the terrorist's modus operandi and was coined in the 1990s by white supremacists Tom Metzger and Alex Curtis. The Lone wolf acts alone and commits violent crimes for tactical reasons. The Lone Wolf is not considered a member of a sleeper cell. A member of a sleeper cell is an infiltrator of the targeted society or organization and remains inactive until ordered to act by a group or organization. A Lone Wolf, this one is an autonomous individual who, is embedded in the targeted society and is capable of self-activation at any time. Other terms have been used to describe similar or comparable forms of political violence, including "leaderless resistance" and "independent terrorism" (Kushner, H.W., 2003: Kaplan, Jeffrey, 1997).

The “Lone Wolf” operated successfully both inside and outside the United States. There are many infamous examples in the United States, Israel and Europe. The case of Baruch Kopel Goldstein, American-born Israeli-American mass murderer, religious extremist and doctor responsible for the deaths of 29 Muslims in 1994 while praying in the Cave of the Patriarchs in Hebron; there is also the case of Austrian Franz Fuchs, who used letter bombs to kill 4 people and injured 15 others.

This other emblematic and not negligible, case is that of US Army Major Nidal Malik Hasan, accused of a mass shooting at Fort Hood in which 13 people died and 30 were injured; or the case of the American mathematician Theodore Kaczynsky, also known as the “Una Bomber”, who carried out a series of postal attacks which left three people dead and 23 injured.

Other emblematic cases to take into consideration and worth mentioning are the cases of political assassinations carried out by lone wolves who assassinated political leaders, such as the case of Yigal Amir, the assassin of the former Prime Israeli Minister Yitzhak Rabin; the case of Volkert van der Graaf, who killed Dutch politician Pim Fortuyn; and the case of Mijailo Mijailovic, responsible for the death of Swedish Foreign Minister Anna Lindh. These acts of violence provoked by “lone wolves” illustrate the numerous differences in targets and methods of operation, as well as the diversity of political or ideological origins of the perpetrators

Al-Qaeda (Afghanistan)

Al-Qaeda is one of the terrorist groups of modern times considering the history of the formation of this organization. It has become the dominant force in the global extremist movement due to its ideology, goals, and strategy. Al-Qaeda's strategic goal is to unite all foreign fighters in the global extremist movement. Local concerns over the problems of global jihad have prompted Al Qaeda to enter into lasting alliances in several countries and regions.

Islamic State in Iraq and Syria (ISIS)

The Islamic State of Iraq and Syria (ISIS) is a radical Sunni Muslim organization that intends to restore an Islamic state, or caliphate, that encompasses parts of Syria, Lebanon, Israel, Jordan, the Palestinian territories, and southeastern Turkey and to expand its influence on a global scale. The Islamic State has alternated between three combat strategies: conventional, guerrilla, and terrorist.

Boko Haram (Nigeria).

Boko Haram is an Islamist movement founded in 2002 by Yusuf Muhammad in Borno State, northeastern Nigeria. The group's initiators intended to eradicate corruption and injustices in Nigeria, influenced by Western customs, and impose Sharia, or Islamic law. The group radicalized and vowed to avenge the death of its founder Yusuf and members of the group, killed by security forces in 2009. Later, the group branched out under the ideology of other terrorist groups such as Al-Qaeda and ISIS. Concerning the terrorist threat in Africa under the aegis of Boko Haram, the terrorist threat is not monolithic but rather made up of a great diversity of distinct entities. These groups are geographically focused on territorial or political objectives. These groups, in order of lethality, include Boko Haram, Al Shabaab, groups linked to ISIS in North Africa, Al Qaeda in the Islamic Maghreb (AQIM), and groups focused on the Sinai.

Biometric Identification

The purpose of biometric identification is to determine the identity of an individual. In the main objective of biometrics, the need is to capture a piece of biometric data of the targeted person. One of the attractions of biometrics is that the body is thought to provide an objective and incontrovertible source of truth about a person’s identity (Martin, Aaron & Whitley, Edgar. 2013)

Identity theft, terrorism and cybercrime, changes in international regulations, have prompted the emergence of the new biometric security solution. The security sector has long used biometric systems for the prevention and fight against terrorism, and which received special attention from the United Nations Security Council by its resolution 1373, because of the attacks of 11 September (S/RES/1373 2001).

Biometrics can be defined as the most convenient way to identify and authenticate individuals through unique biological characteristics reliably and quickly. Fingerprint scanners and cameras at border posts capture information that helps identify travelers entering the country more accurately and reliably. According to John Wagner, executive assistant deputy commissioner at the U.S. Department of Homeland Security, Customs and Border Protection (CBP), John Wagner has said that, more than 43.7 million people had been scanned at border crossings, departing cruise ships and elsewhere so far. This process helped prevent 252 people from attempting to use another person's passport to cross the border (Venture Feb 6, 2020).

Biometric data, political opinions, and genetic data uniquely identify a natural person. These data are “sensitive” and subject to a strict legal framework because they have the particularity of allowing the identification of the person at any time based on a biological reality that is specific to them, permanent over time, and of which they cannot free themselves.

Nature of the Study

Many scholars have already carried out work on unclassified cases and analysis of government reports on the subject of intelligence and terrorism, but few on the overall aspect of intelligence and counterterrorism. This study will examine in the context of counterterrorism and intelligence, money laundering, methods of terrorist operations, biometrics, the intelligence cycle, and the different intelligence systems of U.S. allied countries in comparison with the U.S. security system.

Relevance and Significance of the Study

The impact of the ramifications of terrorism across the world is due to the draconian measures put in place in the United States after the events of September 11 to protect the American nation. The establishment of a counterterrorism intelligence system will be proposed, in order to find convincing factual evidence in favor of the creation of a new counterterrorism intelligence structure, which therefore constitutes the key element of this study.

This study will also show how terrorists immigrated to several regions and how local groups pledged allegiance to their leader and their group's ideology. As technology has evolved, many people easily commit crimes due to the anonymous nature of the Internet. Terrorists practice cybercrime and radicalize people who succumb to their speeches. Computer crime and digital evidence are on the rise (Hobbs et al. 2014).

This study needs to be taken into consideration, due to its revealing nature of the permeability of the borders of allied countries by terrorists and the weakness of current intelligence structures in allied countries to protect against the invasion of terrorist sleeper cells that engage in money laundering, drug trafficking, and other violent crimes.

Terrorism, counterterrorism and intelligence are linked to this study because the sources of information used by both terrorist and counterterrorism agents come from same intelligent sources. Information gathered through espionage, images obtained by satellites orbiting the Earth, intercepted communications, and even publicly available media reports are used by both terrorists and intelligence agents. There are many crimes committed online, such as the use of confidential access codes, computer hacking, computer sabotage, child pornography, cyber-harassment, etc.

However, in a changing world, with advanced technologies, all information about individuals can be found on the web. Searching becomes easier with techniques like code analysis, biometrics, and artificial intelligence. What favors crime committed on the Internet is its anonymity, its globalization, its speed of diffusion and above all the fact that the Internet remains in a cross-border space where there is no appropriate legislation or international agreements (Kim et al. 2011).

The impact of cybercrime on individuals who may have been radicalized cannot be ignored. All sectors of society must be proactive in protecting themselves against cybercrime attacks. Cybercriminals relentlessly seek to steal valuable information from Open Source Intelligence (OSINT), which could lead to disastrous consequences. Therefore, the state and individuals should stay vigilant and take necessary measures to safeguard digital assets. The United States should find a way to mitigate cybercrime in allied countries and effectively promote the security of allied intelligence services (Jahankhani et al. 2014; Staniforth 2014).

The study will be discussing on lone-wolf terrorists which will include their reasons for radicalization, the inspiration behind their violent intentions, and the message they aim to convey through their attacks. The threat of lone-wolf terrorism is a complex challenge that cannot be ignored. However, terrorist specialists can overcome it by identifying the reasons behind their radicalization at the earliest possible stage. Lone wolves operate independently, without any directives or known hierarchy, making it imperative for officials to remain proactive and stay one step ahead of these individuals. By doing so, the official terrorist specialists can effectively deprive them of the means to commit heinous acts and protect the communities from their destructive actions.

Organization of the Study

The inclusion of this component in the thesis is paramount. Its illuminating nature serves as a beacon for readers, guiding them effortlessly through the research and its results. The design of this element is such that readers can easily imbibe the content of the thesis, using it as a roadmap to gain a better understanding of the research.

This fascinating study is divided into five chapters that delve deeper into the complex context of terrorism and intelligence.

Chapter I set the scene by presenting the challenges associated with terrorism in the areas of intelligence, global security, and counterterrorism. This thought-provoking presentation of the issues is designed to lead the public to a key research question that will lead to important knowledge in this critical area. Thus, by presenting the issues, a research question was formulated.

Chapter II of the literature review will discuss theoretical frameworks and ideas on intelligence and terrorism in a counterterrorism context. All topics relating to this study will be explored, including the theme of terrorism, counterterrorism, the use of OSINT, biometric border detection technology, the domestic intelligence agencies of various U.S. allied countries, tracing their creation, current structure, successes, and challenges, the expansion of terrorist groups, methods of collection, the role of OSINT, and illegal distribution of information on the web, films, music, software, and illegally copied documents that show examples of Internet crimes that amplify the impact of crime (Hobbs et al. 2014).

Chapter III This study is dedicated to examining the design and methodology of this research work, which aims to explore the form of a new structure. To support this study and make it more comprehensible, the author will be presenting some emblematic case studies. Among these cases, this research work will highlight the lack of effective counterterrorism structures in U.S. allied countries. This will help to illustrate how terrorists have been able to infiltrate different regions unnoticed and aims to shed light on the importance of having strong counterterrorism structures.

Chapter IV will discuss the case studies on domestic intelligence agencies in the context of counter-terrorism in the United Kingdom, the United States, and the Democratic Republic of Congo in Africa. Combating terrorism is a complex and ever-evolving challenge, and every country faces unique obstacles in tackling it. In the United Kingdom, the United States, France and the Democratic Republic of Congo, the approaches taken by domestic intelligence agencies differ significantly. Given the intricacies of this new science, countering terrorism requires a strong combination of military force, diplomacy, and a deeply committed policy that respects the intelligence cycle's principles. By recognizing the importance of these factors and working collaboratively to develop effective counterterrorism strategies, this study can help prevent future attacks and promote a safer, more secure world.

Chapter V is an essential part of this research, as it presents the findings, conclusions, and lessons learned from case studies. Based on this research work, this study highly recommends that allied countries establish a “domestic counterterrorism” structure. This approach will enable countries to better address internal security threats and reduce the risk of terrorist attacks. This study strongly urges policymakers to consider its recommendations and take the necessary steps to implement this structure.

CHAPTER TWO

LITERATURE REVIEW

Introduction

This part of the thesis highlights the need to strengthen the protection of U.S. allied countries, which work in concert with the U.S. government for global social, economic, political, and security interests.

In the literature review on intelligence and terrorism, the elements that highlight the indelicacy of intelligence and counterterrorism services are data breaches, unprotected open network sources, and emerging biometric tools that affect their intelligence operations. These critical factors are known as biometrics and artificial intelligence, which support the detection of authorized personnel who may conduct counterterrorism operations in the U.S. and abroad. Terrorists pursued in the U.S. take advantage of the permeability of weak borders and the absence of domestic counterterrorism policies in these less protected U.S. allied states.

The nature of the study being academic presents the majority of the work which is firstly based on a review of the existing scientific and expert literature on the three main domestic axes and areas of the study which are intelligence, terrorism, and counterterrorism. All types of academic work are recorded analytically and qualitatively, and in a non-exhaustive manner, so that it is illusory to account for the entire corpus: theses, works, articles, and dissertations.

This research will use case studies to explore all the elements that will help answer the research question as it is of paramount importance to not only get the answer to the research question but, to offer the United States and its allied’s decision-makers solutions to protect the private information of their authorized personnel who work to combat terrorism.

According to Mintzberg (1979), it is important to construct a theory going from the research question to the case study, because whatever the size of the sample taken or the interest, the objective is to systematically collect specific data types (Mintzberg 1979.585).

It is important to mention in this section that, the internet has diverse amounts of information from the services offered on the web, which has led to an evolution of an increasing mass of digital data that may be used by enemies and the authorized personnel. The information on the web is needed for business, education, research, and military planning (Pune 2020).

From historical and comparative perspectives, reviews of the consequences of counterterrorism will present thematic analyses as well as case studies from the United States (U.S. Intelligence Community), Europe (Great Britain with "MI6 - Military Intelligence), France, with "SGDN - National Defense General Secretariat") and the case of the Democratic Republic of Congo in Africa with (ANR – National Intelligence Agency). Taking the example of African countries, all their intelligence systems are diversified but all have been initiated by the colonists who weakened them at will after the era of African independence for the economic interests of the metropolis. The subject of this literature review addresses terrorism and intelligence, which demonstrates the permeability of the borders of countries allied to the United States. One of the contributors, John Finn, compares post-9/11 counterterrorism legislation in the United States, Europe, and the East to demonstrate the effects of hastily crafted policies on civil liberties. Gallya Lahav also shows how immigration policy has become inextricably linked to security in the EU and compares the European fear of internal threats to the American fear of external threats during 9/11. The case study will examine why the Congolese response to terrorist threats has not become even more coercive over the past twenty years, even though the Democratic Republic of the Congo is one of the members of the United States allied countries.

Research topic in the Literature Review

Three research themes will be addressed in this work which is in particular Intelligence, Terrorism, and Counter-terrorism. The interest of this work is keen to scrutinize current intelligence structures, terrorist groups, and counterterrorism to demonstrate how this topic affects global security and the need for a domestic Counter-terrorism structure. These themes are chosen because of their interconnectedness and will be examined as follows:

First: Review of intelligence literature.

It is necessary to understand that intelligence operates differently in colonized countries compared to metropolitan countries. The intelligence agencies of old democracies such as the United States, France, and Great Britain are equipped to protect their respective states. On the other hand, in developing countries, intelligence services should ideally work for the state, but in the context of colonized states like African countries, they often collaborate with the power in place rather than the government. It is essential to note that there is a difference between the state government and the power in place. Those who exercise power are not working for the benefit of their state due to the presence of spies and the mafia (Nicolas Beau, Olivier Toscer, 2019).

Under these conditions, the intelligence services are only there to inform their friends at the top of power. This is extremely worrying because there is a large parallel distinction between the political policing of colonized developing countries and that of metropolitan countries. This type of practice poses obvious problems that impact the way the security of country is managed. The intelligence services used by the regimes in place have very specific missions. Officially, they act within the framework of the rule of law, but in reality, they often commit malfeasance. Westerners who colonized African countries trapped African intelligence services by deactivating all the elements of intelligence collection which are the equipment that allows good analyses and good operations to be carried out. Once information collection is poorly equipped and intelligence analysis and operations will not be satisfactory. There is a deep reason which explains this inefficiency of the intelligence system of developing countries. The colonizing countries did not choose to grant independence to developing countries but were forced to do so by violent emancipation movements. Each country in the metropolis begins to seek to maintain its influence over its former colonies. This maintenance of the influence of metropolitan countries implied placing their agents at the head of government to control the economic resources of developing countries (Aly, H., 2022).

Even if colonization is no longer visible in the administration and army of newly independent countries, the intelligence services of Western countries have secret missions to manipulate their indigenous agents in power who work indirectly for the metropolis. These secret services of the metropolis pull the strings behind the scenes and destroy the intelligence systems of newly emancipated countries for economic reasons. (Henry Laurens, 2011/2).

The European capitals, understood the arrival of the independence of the colonized countries, instead tried to control the process of emancipation, while giving them a semblance of independence which would not be profitable by deactivating the principles of collection and dissemination of intelligence, thus making the analysis of the intelligence systems of colonized countries ineffective.

Unfortunately, with the rise of terrorism and despite the voluntary weakening of the intelligence and security system by developing countries, formerly colonized countries have today become allied countries of Western countries and must integrate into the maintenance of global protective operations to counter the spread of terrorism and block further influence from China, Russia, North Korea, and Iran.

This difficulty in losing the economic advantages of developing countries does not allow Western countries to think about reforming the intelligence systems of underdeveloped countries.

Generally speaking, the end of the 21st century has been marked by a transformation in the role of secret intelligence services in international politics. Intelligence and security issues are visible in Western political discourse as well as the broader public consciousness. Public expectations for intelligence are high, and these demands include much greater disclosure of previously secret knowledge. Much of the effort to educate communities about their security is attributed to the shock caused by the terrorist attacks of September 2001. These events highlighted the vulnerability of Western societies and the importance of having reliable information about threats to terrorists. As Christopher Andrew points out in his contribution to this collection, the threats posed by Osama bin Laden and Saddam Hussein succeeded in transforming the British government's policy on the public use of intelligence (Christopher Andrew, 2004).

In public opinion, Prime Minister Tony Blair and President George W. Bush were widely accused of deliberately distorting intelligence information to justify their decision to declare war on Iraq in April 2003, which is considered an intrusion and aggression against an independent country. Understanding of the intelligence process and its importance to national and international security policy has never been clearer. Understanding intelligence in the 21st century draws on its cycle, the model of information collection, and its evolving role in national and international politics (Len Scott and Peter Jackson, 2004).

According to Sherman Kent it has been over fifty years since intelligence was first considered an interesting subject worthy of serious academic study with the publication of Strategic Intelligence for American Foreign Policy (Sherman Kent, (1949).

The study of international security is increasingly influenced by understanding the role of intelligence in policymaking. Both eminent British historians specialized in the literature relating to intelligence studies and international relations and were able to describe intelligence as the missing dimension of international affairs (Christopher Andrew and David Dilks,1984).

Christopher Andrew continues to argue that intelligence still does not have its rightful place in Cold War studies, even though it was during this period that HUMINT was frequently used in combination with espionage practices to accompany targeted assassinations. people. The literature on the Cold War period is truly insufficient. » (Christopher Andrew, 2000)

Andrew argued forcefully and convincingly in his collection that the overarching subject of intelligence during the Cold War demonstrated that it was impossible to dispense with intelligence as a particular and potentially crucial subject of historiography. (Andrew, 2001)

John Ferris, R.Boyce and J.Maiolo, (2003), offer a different view, believing that "intelligence is not a form of power but a means of guiding its use, whether as a combat multiplier to help understanding how to apply force or how to resist and persist". How to define intelligence works if it asserts itself as a force to help political leaders have good judgment and a good understanding of events, which is more crucial (Christopher Andrew, 1995).

The intelligence process becomes a collection of information from government agencies only, if the stages of the intelligence cycle include the issuance of requirements by decision-makers, which develop through collection, processing, analysis, and the publication (i.e. dissemination) of information. The circuit is completed when decision-makers provide feedback and revise the requirements. (Michael Herman, 1998)

Assessments written by intelligence agencies are typically based on a combination of secret and open-source information. Since not all of these activities can reasonably be defined as intelligence activities, this suggests that the essence of intelligence assessment (Herman, 1993)

Globalization has influenced the domestic security of US-allied countries, including advances in information technology, which have introduced new challenges that require new solutions. There are, however, remarkable parallels between the debates over Pearl Harbor and the aftermath of 9/11. In both cases, the emphasis was on lessons learned and policy prescription. Several very similar themes demonstrate the inability to conduct effective espionage against a racially or culturally “foreign” adversary; the inability to organize and coordinate the collection and analysis of information between departments; the lack of resources to collect, translate, and analyze intelligence and, finally, the inability of political leaders to understand the value and limitations of intelligence due to the disruption and hasty reorganization of the United States to protect against terrorism. The publication in 1946 of the lengthy and detailed Congressional report on the attack on Pearl Harbor provided the primary raw material for one of the founding texts of intelligence studies (United States Government, 1946).

Roberta Wohlstetter's work on the Port Attacks: "Warning and Decision" demonstrated the rich potential of an interdisciplinary approach to the study of intelligence and policy making (Roberta Wohlstetter, 1962).

Debate on Domestic Intelligence: Sullivan, JP and Lester, G. (2022) were able to ask the question of what domestic intelligence is. This question is recurring and tends to arise after a security crisis or a significant threat. The contemporary debate over domestic intelligence and all its ramifications was catalyzed by the attacks of September 11, 2001, which exposed the United States to the threat of global terrorism (Rohini Kuruo and Benjamin Wittes, 2021)

The attacks gave rise to a series of new approaches to law enforcement-intelligence relationships and challenged the conventional idea that different levels of intelligence and law enforcement should interact with each other in the United States. Given that 9/11 is widely described as an intelligence failure, it is natural that an examination of the structure of intelligence, both foreign and domestic, and across these divisions, has taken place. (Sullivan, J.P. and Lester, G., 2022).

The domestic intelligence debate has arisen again in light of the January 6, 2021 insurrection, when Trump supporters attacked the Capitol in an attempt to prevent the certification of newly elected President Biden. While the insurrection has raised many political questions, it has also once again raised the specter of a failure of law enforcement and domestic intelligence to share the evolution of American domestic intelligence since 9/11.

The Light of the Capitol Attacks also reviews the literature and practice of intelligence reform in the context of foreign comparative experiences (France, the United Kingdom, and the Democratic Republic of Congo). It appears that despite fusion centers and contemporary models of U.S. domestic intelligence, domestic intelligence reform remains necessary in U.S. allied countries. Rohini Kuruo and Benjamin Wittes (2021) discussed the January 6, 2021 attack on the United States Capitol, which exposed flaws in the United States' domestic intelligence system. Although the full story has yet to be told, early reports suggest a breakdown in threat assessment and interagency communications. (Claudia Grisales; 2021)

Indeed, some officials attribute operational deficiencies to intelligence failures, particularly in sharing threat intelligence between agencies. There were several agencies dealing with domestic intelligence without there being good communication between all these agencies (Rachael Levy and Siobhan Hughes, 2021).

A comprehensive assessment of the intelligence function and operational facets of the insurgency response, both to the immediate attack and to the conditions preceding it, is warranted (Ryan Goodman and Justin Hendrix, 2021).

Many questions remain. Was the event a failure of the intelligence services? If yes, of what nature: is it an operational failure or a failure of operations-intelligence fusion (Rohini Kurup and Benjamin Wittes 2021).

Although preliminary investigations have shown that the flow of information between agencies is far from perfect, the overall operational dimensions of these transactions have not yet been fully assessed. To this end, some analysts, such as Brian Michael Jenkins, have suggested the creation of a national commission to investigate the attacks (Brian Michael Jenkins, 2021).

Although efforts to form a 9/11 style commission failed due to partisan resistance, there remains a need to address the still-unresolved foundations of national intelligence. For this assessment, this article provides an overview of the story. The U.S. domestic intelligence context defines the scope of the domestic intelligence enterprise and assesses post-9/11 reforms. Finally, he shares foreign perspectives on intelligence to inform current and future debates (Karoun Demirjian, 2021; National Commission, 2004).

Debate on Counterterrorism Agencies: The debate surrounding the counterterrorism agencies in various countries such as the United States, Europe, the Middle East, and Africa has highlighted some gaps in their ability to protect themselves. The issue of global insecurity affects all nations and should be considered by each of them. The world is divided into two blocs, one comprising the United States, Europe, and allied African countries, and the other consisting of China, Russia, Iran, and North Korea's paranoid regime.

According to the CIA report, the most significant challenges faced by the world are the war in Ukraine and Russia's aggressive behavior, which frequently involves the threat of nuclear weapons and an increase in cyber-attacks. The American intelligence community is worried about China's future conflicts and its weapons and new technologies, for which it is carefully preparing. The CIA also highlights the detrimental role played by Iran, which is attempting to extend its influence over the Gulf regions.

United States: Intelligence Community (IC): The U.S. Intelligence Community is comprised of 18 agencies and organizations, including the Office of the Director of National Intelligence (ODNI). These agencies operate within the Executive Branch and work together to collect and analyze intelligence that is essential for conducting foreign relations and ensuring national security. (Flanagan, S. J., 1985).

The intelligence agencies within the United States Intelligence Community (IC) are described as follows:

► **Two independent agencies**: The Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA);

► **Nine Department of Defense elements:** The Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial- Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the five DoD services; The Army, Navy, Marine Corps, Air Force, and Space Force.

► **Seven elements of other departments and agencies**; The Department of Energy's Office of Intelligence and Counter-Intelligence; the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence; the Department of Justice's Federal

Bureau of Investigation and the Drug Enforcement Administration’s Office of National Security Intelligence; the Department of State’s Bureau of Intelligence and Research; and the Department of the Treasury’s Office of Intelligence and Analysis.

Challenges for the Intelligence Community (IC): The economy, crime, terrorism, and technology constitute the basis of the four major challenges facing the U.S. IC in the current context.

The first challenge is the growing demand for business intelligence. This information may have various national security applications.

The second challenge is that the IC will need to prepare to deal with the problems of transnational organized crime.

The third challenge is that the global war on terrorism has entered a new phase. Groups such as ISIS have lost the territories they controlled in the Middle East but have immigrated to Africa and are now emphasizing their ability to strike Western assets.

The fourth challenge is the IC's need for a more effective collection and analysis cycle that can include other U.S. allies and create a counterterrorism and global security system (Christopher R Moran, Joe Burton, George Christou, 2023)

Europe: Great Britain with “MI5 and MI6: MI5 is the British security service whose mission is to combat security risks in the United Kingdom, while MI6 works overseas to gather information on other intelligence threats and to protect countries against global infiltrations. Comparing the two agencies, the FBI and the CIA in the United States, one of which is for domestic intelligence and the other for international intelligence, these two institutions collaborate to secure their own countries (Phythian, M., 2009)

The term “MI” stands for military intelligence. Thus, MI5 investigates matters of British national security, terrorists and counter-insurgency, like the American National Security Agency (NSA). MI6 (currently called SIS) gathers intelligence on the UK's international affairs, such as espionage in Iraq. Equivalent to the Central Intelligence Agency (CIA), The National Criminal Investigation Squad (NCIS), MI5, and MI6 are made up of high-ranking police officers.

Challenges for Great Britain with “MI5 and MI6: In Great Britain, the isolated fight against terrorism should adapt to the changing nature of terrorists, requiring increased efforts with other countries to establish a comprehensive security system that forms the pillar capable of preventing any terrorist attack (Basu N., 2021).

France: The General Directorate of Internal (DGSI) and the National Defense General Secretariat (SGDN): The General Directorate of Internal Security (DGSI) is the only specialized French intelligence service reporting to the Ministry of the Interior, within the national intelligence community. Given the episodes of political violence that have been occurring continuously for several years, the police in France have invested in anti-terrorism. Unlike Germany and Great Britain, where counterterrorism policing is distinct from regular police activity, domestic intelligence is becoming a specialized police service (Bonelli, L., 2023).

The General Directorate of External Security (SGDN), subordinate to the Ministry of Defense, is responsible for military intelligence and it is also responsible for counter-espionage outside the territory's borders. The DGSE was born from the integration of the various French intelligence agencies of the Second World War. The Free French Forces created in 1942 the Central Bureau of Information and Action (BCRA), which was established in Algiers under the name of the Directorate General of Special Services (DGSS) renamed the Directorate of Studies and Research (DGER).

Consequences

Given the urgency and trauma caused by previous political violence that erased the other activities of these professionals, such as political surveillance and counter-espionage, counterterrorism becomes the main source of legitimization due to current public debates at the political champion. This police force, specialized due to political debates, does not take into account respect for the rights of refugees and immigration laws. There also seems to be a weakness in this specialized policy since its action is concentrated without taking into account the creation of an international network to counter terrorism.

Africa: Democratic Republic of Congo: (ANR – National Intelligence Agency)

The structure authorized to fight against pure terrorism is absent despite the presence on Congolese soil of terrorists active in the east of the country. Counterterrorism only exists in terms of collaboration with almost non-existent structures. In addition to other intelligence missions, the ANR collaborates in the fight against drug trafficking, fraud and smuggling, terrorism, economic crime, and all other crimes constituting a threat to the State or humanity.

The Debate on Foreign Intelligence: History records that foreign intelligence has played several roles, not only during the Cold War but up to the present day. This topic has not received enough scientific attention that it deserves. The following literature provides a general overview of some of the new publications and documentation on Cold War-era foreign intelligence, as well as key dimensions of the subject. There remain, however, persistent obstacles posed by the secrecy and mixed reliability of sources, and the dissemination of an enormous volume of new archival material in the post-Cold War era that has opened new opportunities for studying the role of foreign intelligence in the Cold War (Raymond L. Garthoff, 2004).

When Edward Snowden, who was a contractor for the National Security Agency, disclosed a vast amount of information about secret intelligence-gathering programs that had been implemented under the Foreign Intelligence Surveillance Act in the summer of 2013, American surveillance activities were brought to the forefront of public debate. This debate included the question of how to reform the Foreign Intelligence Surveillance Court ("FISA Court"), the secret court created by law that reviews government applications to conduct surveillance in the United States (Berman, Emily 2016).

The Intelligence Community (IC) is an expert in collecting foreign intelligence outside the United States and is not interested in how to exploit domestic foreign intelligence, largely due to conflicting narratives within the community and which will need to be corrected in the future.

Many elements of the U.S. intelligence community (IC) focus on foreign intelligence collection, in all its forms, outside of the United States. The CI configuration does not address how to exploit foreign intelligence in the domestic context. This is a significant failure because the United States has a home-field advantage in collecting data that can provide U.S. policymakers with a unique information advantage, but this advantage is not shared with the allied countries on which the United States should rely in case of failure, and in case of need for a coalition of forces necessary for the conflict. The FBI can address the internal deficiency of the problem, but not the external deficiency. Domestic intelligence reform is necessary to calibrate the national intelligence framework to address the emerging and evolving threats faced internally (Sullivan, J. P., & Lester, G., 2022)

Second: Review of Terrorism and Open Source Literature

This part will assess terrorism and the impact of open-source intelligence when used by adversaries against the United States. This assessment will include instances of the Islamic State of Iraq and Syria (ISIS) using social media to target U.S. military personnel, particularly in the case of Robin Sage, who opened an account on the social network LinkedIn, using fake IDs to interact with other networks members, and while denouncing US-sanctioned professionals in government and industry. Terrorist groups with expansionist ideology will be examined.

Terrorist groups of interest are Al-Qaeda and ISIS (Islamic State of Iraq and Syria), Boko Haram – al Shabaab, and Al-Qaeda in the Islamic Maghreb (AQIM).

Concerning the terrorist groups al-Qaeda and ISIS from an ideological point of view, these two terrorist entities wish to implement a strict version of Sharia law that all Muslims must respect to facilitate the reconstitution of the caliphate, i.e. -say a territory under authority. of a caliph who assumed the role that Muhammad occupied as a political leader. Once the caliphate is established, all those who challenge it will be eliminated, including the political, social, and religious systems, so that the caliph will dominate humanity and be the leader of all Muslims.

Ideologies – Politic and Strategies: Al-Qaeda and the Islamic State.

The terrorist group Al-Qaeda: follower of the Maoist revolutionary strategy Based on the theories developed by Mao Tse-Tung, the Maoist revolutionary strategy advocates political interference in military actions to convince and unify the population to establish solid operational and logistical support. Once this first step has been taken, a gradual expansion is initiated to strategically increase the available forces to an optimal level to finally quickly attack the enemy.

The terrorist group Islamic State: inspired by the Focoist revolutionary strategy Supported by Ernesto “Che” Guevara, the Focoist revolutionary strategy is characterized by taking significant risks through the massive use of violence to inspire collective support and, at the same time, suddenly destabilize the political system and the leadership in power.

Terrorists immigrated to Africa and managed to ally themselves with local groups. West and Central Africa continue to suffer the terrible consequences of terrorism. The terrorist group like Boko Haram has become the deadliest terrorist organization in the world, responsible for 6,000 casualties in 2015 alone. This terrorist group also contributes to political instability and undermines economic gains and future development. In today's globalized world, it has been demonstrated that a regional terrorist threat can quickly become a global threat. The international community must work together with West and Central Africa to deprive terrorist organizations of their funds and deprive them of the ability to finance terrorist attacks.

Open-Source Intelligence (OSINT): Several searches are carried out on the Internet using a search engine, which is an online tool designed to find websites on the Internet based on the user's search query with the objective of finding the results in their own database, sorting them and compiling them on an ordered list. This list is called a Search Engine Results Page (SERP).

OSINT techniques appeared before World War II known as open intelligence. The enemy press as well as the press of countries that have remained neutral may have been at the origin of the violation or the disclosure of information (Kott 2018).

The number of people connected to the Internet is huge and the link with this number is that the compromising information of each other can be disclosed, because the Internet is one of the open sources that OSINT analyst uses to collect the information.

According to Roser et al. (2019), the number of Internet users increased from 413 million in 2000 to over 3.4 billion in 2016. In January 2021, there was a huge increase in the population accessing the internet with around 4.66 billion active internet users worldwide. This represents a net percentage of 59.5% of the world's population. 4.32 billion of the population have access to the Internet via mobile devices (Johnson 2021).

The availability of highly accurate information compiled in easily searchable places on the Internet about government employees and private sector contractors has increased exponentially in recent years as the popularization of the online social network (OSN) and User Generated Content (UGC) have changed to access information on the Internet (Ye et al. 2011).

The use of this information inadvertently or by design jeopardized intelligence operations and OPSEC in general, such as the CIA "rendition flights" where detainees were airlifted to locations in foreign countries under the auspices of reinforced interrogations. The exploitation and analysis of social media have also helped opponents of the US in various ways. Facebook is the most popular social networking site; LinkedIn provides more accurate and centralized biographical data on its users who voluntarily provide it. Adversaries have used this data to accurately identify US cleared personnel working on classified programs, make connections and hypotheses with other cleared personnel, and uncover sometimes sensitive operational data about intelligence programs (Ryan 2009.1).

The Robin Sage experience: In 2009, Thomas Ryan, co-founder and managing partner of Provider, Security, LLC, led the Robin Sage experiment. The social experiment was described in his report "Getting in Bed with Robin Sage," in which he first presented the Black Hat conference results in 2010. The experiment sought to "tap into the foundational levels of information leakage - the output of data due to the unchallenged trust of people (Ryan 2009.1).

The experiment was unique in that it went beyond simply searching the Internet for sensitive information about the US cleared personnel or operations, but instead targeted personnel who support those operations in actively targeting them through a live social media account. Ryan created "Robin Sage," a fictional female character who worked as a Cyber Threat Analyst at Naval Network Warfare Command. Ryan used his fake academic credentials and compelling online background, to include an appealing profile picture and other social media accounts. Facebook and Twitter were used by Robin Sage to interact and collect information about a certain number of DoD and IC seniors. The experiment was so successful that Robin Sage was offered free conference tickets, job opportunities, asked to comment on the DoD policy white papers in courses, and other incentives (Ryan 2009. 1).

Ryan had a very important experience, which was able to successfully prove the concept that a fictional LinkedIn character with additional seemingly compelling social media accounts was successful in attracting, interacting, influencing, and obtaining information from staff in sensitive positions (most of which had security clearances). These interactions, if adversaries had created them, "could have resulted in a violation of several security protocols" and even "violated OPSEC and PERSEC procedures" (Ryan 2009. 2).

Opponents could take the initiative to use this TTP, not only do they intend to influence future policies or publications through their authors, but they would also like to acquire key biographical data that would allow them to target US intelligence personnel who support classified operations. Journalist Steve Hendricks also used, the use of open-source information. He wrote the book "A Kidnapping in Milan" to track down CIA personnel currently living in the US (Hendricks 2010).

The agents that were involved in the kidnapping of Abu Omar in Italy in 2003 were denounced by the Italian authorities' open-source means. As long as open-source remains in use for the public and that other forms of protection have not yet been found, the personnel working in the account of intelligence agencies will require measures of protection on the internet such as the non-use of certain accounts such as Facebook, and other popular media.

ISIS and the Military Personnel: Around March 2015, terrorist groups abroad had started using open source information to target the US armed forces. This group called “Islamic State's Hacking Division” has posted details of 100 US military personnel online (Fantz 2015).

The group acted on behalf of ISIS and quickly disseminated PII information on the internet to provide targeted details to potential lone wolf attackers. Initially, the USG believed there was a cyber-breach of PII; later it was determined by a Daily Beast article that at least two-thirds of the soldiers on ISIS's hit list had been featured on public Ministry of Defense websites, intended to promote the military, and that the list appeared to be a little bit more than a little creative Google search (Youssef 2015).

A CNN article noted that “ISIS operatives and supporters scoured social media sites to try and glean mass data about militaries, even threatened military spouses online "(Fantz 2015).

There is very little that DoD and IC members can do to prevent this, other than limiting the amount of information they post online. There are countless public archive websites available to paid members that offer personal information to DoD and IC members once a person's name is known. It is easy to find people on the internet. Facebook gives movements, photos, and birthdays of individuals. LinkedIn provides professional details about individuals' lives that can facilitate the disclosure of details one would seek to hide from the public (Hendricks 2010).

Real threats weigh on intelligence officials on mission.

The use of biometric detection technology by adversaries at border crossings has become more efficient with the availability of open-source data and authorized community personal information extracted from OPM, United Airlines, Anthem Health Insurance, and the Ashley Madison Adultery website. When aggregated into advanced analytical databases, this data can be used to identify cleared personnel while traveling abroad, who are their associations, health issues, or sexual inclinations. All these raw data can be used by adversaries to develop a strategy to recruit or blackmail the authorized employee to their advantage. Once biometric data are collected and recorded, it is normally a permanent book. This advanced technology makes it more difficult for US Intelligent agents and open industry personnel with security clearances to maintain operational security at border crossings and foreign checkpoints. Technologies have the potential to help others track and distinguish us" (Brannen 2015).

The US primarily uses biometrics at border crossings as well as on the battlefield overseas. Biometric technology is present at almost all national airports and major border crossings. The exact figures remain sensitive data and are not released by the US government. The most common type of biometric technology at US airports and important border crossings is facial recognition cameras. On March 11, 2015, US customs launched a biometric facial screening program at Washington Dulles International Airport, outside of Washington, DC (Aguilar 2015).

As part of a random selection of inbound passengers, customs officials will take a digital photo of the passenger and digitally compare it to the photo on the passport's digital chip. The program of the Biometry generates a number that determined if the passenger need more screening (Aguilar 2015).

This biometric screening technology is mainly used to affirm the person's identity, whose name is on the passport. The use of biometrics can help identify terrorism suspects even with the partial use of a photo and little other evidence (such as in the Boston Marathon bombers).

Adversaries can also use biometrics at the border checkpoints to identify intelligence officers and obstruct their operations. A rare glimpse into the exposure of a classified operation due to biometric identification technology occurred in 2010 when a suspected Israeli Mossad team conducted an assassination mission in Dubai.

Third: Review of Counter-terrorism literature

The literature on terrorism and counterterrorism presents a dominant concern concerning research methodology. It should be noted that terrorism and counter-terrorism are among the most difficult topics to study, due to their dangerous nature. Interviewing active terrorists is very dangerous. There are also clandestine organizations that are not open to terrorism research and do not cooperate. Even if imprisoned terrorists were interviewed, it could not produce the desired results. Intelligence agency files are not accessible until decades later.

In terms of academic disciplines, researchers who have worked on terrorism and counterterrorism have a background in political science, international relations, or security studies. Among these eminent researchers, we can name a few. These are peers Andrew Silke (2019), Boaz Ganor (2005), James J. F. Forest (2015), Martha Crenshaw and Gary LaFree (2017), Robert J. Art and Louise Richardson (2007) and all the others, including well-regarded studies by Daniel Byman, Ronald Crelinsten, Richard English, John Horgan, Bruce Hoffman, Brian M. Jenkins, Clive Walker, and Paul Wilkinson.

Valid reasons for the globalization of counterterrorism.

The armed efforts of terrorist groups such as Al-Qaeda and ISIS are because these terrorist groups continually aim to weaken the United States. These terrorist groups view the United States and its allies as primarily responsible for the rejection of their version of Islam on the international stage and believe that the United States supports corrupt dictators in the Middle East, including the leaders of Egypt, the Middle East and the East Saudi Arabia (William McCants and Clint Watts, 2016).

For terrorist groups united in so-called jihadism, terrorist acts are intended to maintain the momentum of continued war until the Americans are militarily and financially annihilated, their human resources exhausted, and their hegemonic status taken away from them after having been isolated and humiliated. The actions of terrorist groups are not oriented toward the short term since they perceive their conflict with the West as being of an existential, intergenerational" nature (Garrett Pierman, 2015).

The military strategy of terrorist groups consists of establishing several subsidiaries in countries whose population is predominantly Muslim and where their implementation will be supported by the political-military context such as the holding of an insurgency, a weak central government, places uncontrolled or popular opinion against the West, to eliminate Americans (military, diplomats, tourists, businessmen, academics), in Muslim countries since the latter prevent the establishment of the caliphate. The territories conquered by the terrorists are Somalia, Yemen, Syria, Northern Pakistan and ungoverned territories in Africa, like Libya, Mali, and the Eastern Democratic Republic of Congo to be used to launch attacks.

Indelicacy of Intelligence and Counterterrorism: An Exploration of the Evidence.

In countering terrorism, intelligence plays a vital role but can be weakened by data breaches, unprotected open network sources, and biometric tools. About the Open-Source, the U.S. government benefits from the distribution of all information on the Internet and easily accessible technology to accomplish its daily tasks. Unfortunately, the U.S. government does not have a good policy in place to implement appropriate and up-to-date safeguards to protect authorized personal information, despite the Federal Trade Commission Act (FTC Act), which is used to prohibit unfair or deceptive commercial practices involving the collection, use, processing and disclosure of personal information (Federal Trade Commission Act of 2006).

According to Carcaño, what makes OSINT more vulnerable is that the information is a public source and its content is commercialized or free. These may be documents of any content, in any medium, under any means of transmission or mode of access (Carcaño 2020).

This emblematic case is cited as an example which weakened States and strengthened its allies who were not equipped with the necessary means of defense. The Office of Personnel Management (OPM) data breach resulted in the highest quality and largest quantity of personal information from U.S. security.

Data breaches concern and include information on authorized U.S. personnel's families, overseas contacts, foreign travel, home address history, educational history, divorces, bad habits, records judicial and other sensitive information that can now be used by opponents to target and exploit them. The counterintelligence consequences of this breach against the U.S. government's most sensitive employees are unprecedented. The use of this personal information and its combination with OSINT and other data breaches (such as airlines, health systems, and Ashley

Madison's adultery website, to name a few a few) would paint an almost complete picture of habits, habits and travels operational details that may correlate with intelligence operations in the adversary's country.

This data, when properly captured in state-sponsored biometric detection systems at border crossings, could potentially be used to identify or flag authorized U.S. personnel transiting certain OCONUS countries. Exposure to authorized personnel has long-term negative consequences and directly impacts the effectiveness of intelligence operations that authorized U.S. personnel conduct abroad.

Biometric Recognition: It is also important to mention in this section that automatic recognition has been applied to identify criminals, track patients in medical IT and personalize social services, similarly this automatic recognition has been installed to identify individuals depending on their biological behavior. This method is likely to identify both terrorists and authorized personnel. Efficiency of access and protection of use of services should be increased (Lee Gomes 2001).

Biometric technology is evolving rapidly and OSINT is accessible over the Internet. Through this method put into practice, the public has been exposed to biometrics largely as a high-tech gadget in spy thrillers, as a frightening tool of the state, or as a tool for corporate surveillance in the speculative fiction. Facial recognition can be applied to a wider range of applications, including biometric authentication, surveillance security, border control, forensics and digital entertainment. Various technology specializations have been added through artificial intelligence to support technologies related to facial expression, aging, posing, lighting and occlusion. With the growing risk of identity theft, facial recognition is not yet as accurate, flexible, and secure as desired (Huang, Liu, Li, and Li 2015).

Biometric systems allow individuals to be recognized and to view remotely access to physical spaces, information, services and other rights or benefits, including the ability to cross international borders. However, human recognition systems are fallible.

Operation of biometric system

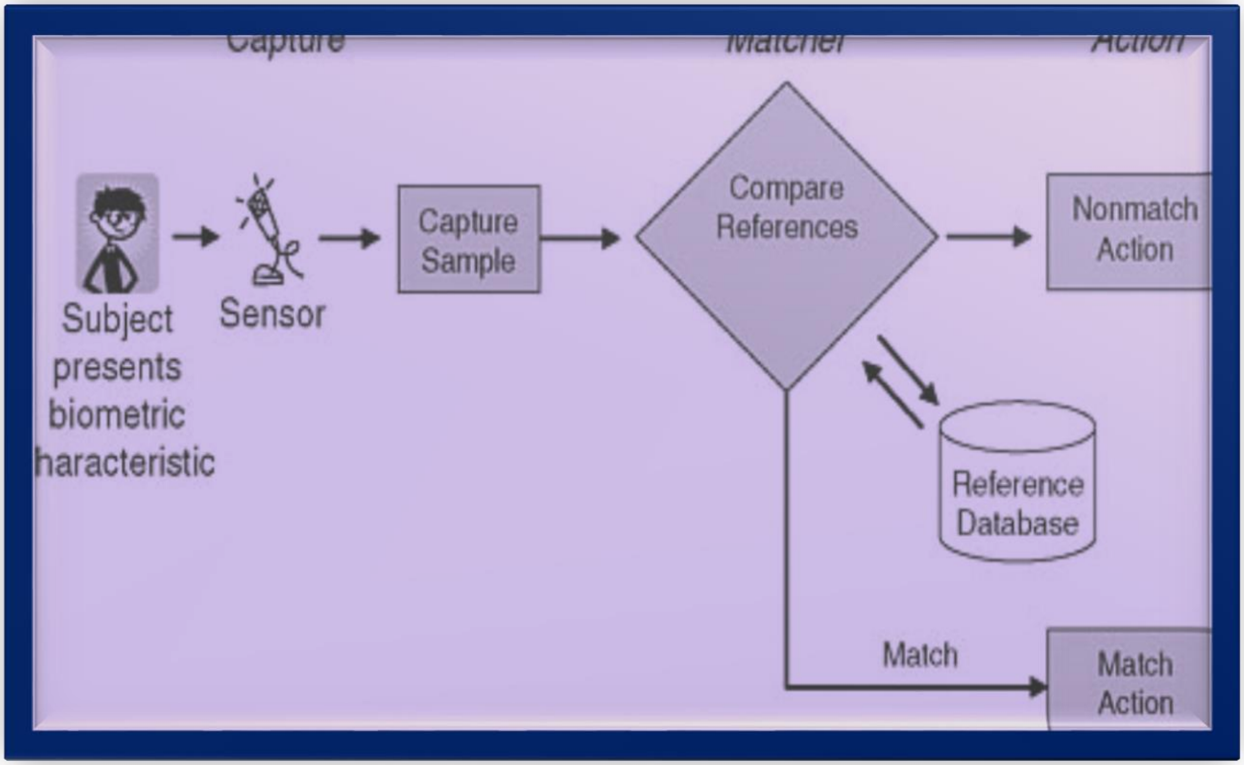


Fig.1: Operation of biometric system

<u>Sources</u>*: Biometric Recognition: The National Academies Press nap.edu*

Figure 1 shows the operation of the general biometric system. There are two basic operations which are carried out to make a general biometric system: the ***“capture and storage****” known as “reference of enrollment of biometric samples". Then, the new captures of the biometric samples will be compared with the first corresponding reference samples called* ***“matching”****. At the end of the process, the “capture and* collection of biometric data" recognize *the subject. "The Referral Database" is where biometric data is stored. And the information collected will be compared with the reference data, to allow the final recognition decision to be taken.*

Assumptions and Limitations

The information of individuals and businesses is easily accessible, which does not spare airlines, the health sector, the hotel industry, banks, and even state institutions, which have become the target of enemies. It is very easy to consult hotel databases through the archives which make it possible to trace or reconstruct the complete itineraries of operational activities, their travel histories, and other personnel movements throughout the world. Travel History is one of the conceptual models that make it possible to reconstruct the trajectory of travelers from recordings of their position and their interactions. Andrienko and Wrobel (2007) use the time method to study the stationary part of a trajectory and argue that the more time a person spends in a place, the more important that place is to a person (Andrienko, Andrienko and Wrobel 2007)

Considering activities such as hotel access, airport access, and credit card usage, beyond this historical data, it wouldn't take much more to create a list of potential targets High Level Value added (HVT) of authorized personnel and industry personnel for potential recruitment, blackmail, or exploitation.

A criminal could take a person's fingerprint on a glass table and then use it for biometric purposes, to access a device or an account. Hackers can also target biometric databases, exposing people to identity-based attacks. When these sources of information cited above are combined, they give adversaries of the United States a clearer picture and understanding of who the cleared personnel are that support these intelligence operations abroad. The US cleared personnel is targeted, when subjected to biometric screening procedures before entering a hostile country.

Theoretical Framework

Introduction

The theoretical framework that will guide this research will be determined by the intelligence cycle. Analyzes of allied government agency collection systems through academic articles will demonstrate the nexus between terrorism and intelligence, and how adversaries abuse biometric technology in conjunction with the availability of OSINT. Since biometrics is inherently public, it could turn out that a third party could duplicate certain traits.

The theoretical framework will demonstrate the absence of appropriate structures or the weakness of the anti-terrorism structures of allied countries, which do not respect the standards of professional intelligence practice within the framework of "security intelligence" and "foreign intelligence".

This theoretical framework will also help to choose a better model of the intelligence cycle, capable of responding to the need to establish a counter-terrorism structure at the domestic level of each country allied with the United States for the global security interest.

These analyses and case studies will help design the framework that will explain the need to create a specialized “domestic counterterrorism intelligence” structure in U.S. allied countries to combat terrorism on a global scale. The current framework is designed on the basis of demonstrating the robustness of a good intelligence cycle capable of dealing with threats due to terrorism, it seems imperative that this intelligence cycle which truly encompasses the entire intelligence process leads to achievable policy outcomes or decisions.

Gill, Peter, and Mark Phythian (2006) recognize the usefulness of the intelligence cycle in explaining the process of "planning and directing, collecting, processing, analyzing and producing from all sources, and disseminating" (Gill Peter and Mark Phythian, 2006)

Lowenthal supports these arguments by going further, using the term “requirements identification” instead of planning or guidance. It adds two more stages to the cycle which include “consumption and feedback”. Discussions about the cycle end with diffusion, and policymakers, after reviewing the product and evaluating their options, can contribute to the evolution of the product. This makes the feedback stage vital and allows intelligence practitioners to assess the expectations of their policy makers and thus refine the intelligence product accordingly (Lowenthal, Mark M., 2015).

The intelligence cycle

The intelligence cycle involves the identification of needs, including collection of information, processing of raw information, analysis of information, dissemination/action, and transformation of information into intelligence. The words information and intelligence have very similar meanings. Intelligence is bringing to someone’s attention while information has the meaning of “action to inform”. The “intelligence cycle” is the preferred tool for understanding the triple mechanism of institutionalization, rationalization, and bureaucratization that the academic and professional literature on intelligence studies (Chopin, O. & Oudet, B., 2023)

The purpose of the intelligence process is to provide policymakers with timely, accurate, and relevant finished intelligence products. While this view sometimes oversimplifies what actually occurs, it is a useful construct for understanding the basic functions that any intelligence enterprise must accomplish to be successful.

Step 1: Requirements

The modern security landscape represents an endless and complex array of information, making it infeasible for intelligence agencies with limited resources to cover every possible threat with equal attention. Thus by necessity, the intelligence cycle begins with a shifting set of requirements that dictate which issues or targets receive highest priority. Depending on the threat environment at any given time,

Requirements II

In the case of the United States, intelligence agencies are separated from the policy process by a semi-permeable boundary, thus giving policymakers the job of setting requirements. In this framework, executive bodies such as the President, the National Security Council, and the Department of Defense are charged with strategically determining these priorities and communicating them to the Intelligence Community in a detailed manner. But are policymakers always active participants in this part of the process? With their own manifold duties and shifting priorities, tasks like requirements setting may easily fall through the cracks.

Requirements III

The success or failure of a set of requirements depends ultimately on the passage of time and the ability of policymakers and their appointed officials to adjust accordingly. As the transition from the Cold War to the War on Terrorism shows, intelligence requirements shift with the geopolitical winds. The single most overriding threat of today may fade to relative obscurity tomorrow, just as the peripheral concerns of the present may become quite threatening in the future.

Insider Threats to Intelligence Operations

Since the end of the Second World War, a manifestation of imbalance has appeared between the funds allocated to the Department of Defense (DoD) and the Department of State. This imbalance is reflected in the concern that is spreading among defense officials and the military community, who have been unable to protect important data that requires high protection. The theft of federal government data related to China could affect hundreds of thousands of military personnel according to a member of the Senate (Wray C 2020).

The literature on the subject of this research shows that this approach has been informative but much more theoretical because few works have used it to address information issues related to the protection of authorized personnel in the United States. Intelligence theft is becoming a very valuable activity in public records to create comprehensive profiles of certain targets and this activity is important to the intelligence community (Bradbury 2011; Steele 2006).

Nexus between terrorism and intelligence

Islamophobia in the context of counterterrorism results from the assimilation that Muslims are the perpetrators of terrorism. This assertion is emboldened by US intelligence efforts to frame them. Some “terrorism experts” have close ties to the U.S. and Israeli intelligence services and therefore closely monitor Muslims. The example of the Holy Land Foundation, a Texas-based Muslim charity run by Palestinian-Americans, has been targeted by both the US state and the Islamophobic industry for its questionable ties to terrorism, while some Americans have long held negative opinions toward this organization. The level of Islamophobia, that is to say, a fear or hatred of Islam, has increased. Negativity in esteem for Muslims has now reached unprecedented levels in the United States.

In the years following 9/11, to create a theory that Muslims were terrorists, the Islamophobia industry's most influential "terrorism experts" were closely linked to the state and participated in the campaign to demonize Muslims. For example, R. James Woolsey, who was the former director of the Central Intelligence Agency (CIA), his stated mission based on tax documents, was to "conduct research and provide training on international terrorism and related issues." while it was among the inventories of the theory "The Muslim is always linked to a terrorist group".

The extent of US spying on Muslims after 9/11 had to be increased and mapped by the US Department of Justice (DOJ), which was able to list Muslims as linked to terrorism to provoke popular debate and invent Muslim terrorists to represent them. The threat embodied by the "war on terror" is something "knowable, exploitable and controllable in a particular form" (Burnett and Whyte 2005)

These "terrorism experts" involved in the rise of Muslim terrorism are described by Nathan Lean (2012) as the "Islamophobia industry" and their direct and indirect links to Israeli and American intelligence services are well documented.

There indeed seems to be support from Muslims in terrorism but this cannot lead to a theory based on the involvement of Muslims at all levels in terrorism. What is true is that scholars of Arab-American studies often cite the invisibility of Arab Americans before 9/11 and their hyper-visibility alongside Muslims after 9/11 (Jamal and Naber, 2008).

How biometric technology is vulnerable and profitable for terrorists.

Terrorists can take advantage of data breaches by hacking them. Biometrics is a pattern recognition system that refers to the use of different physiological traits such as face, fingerprints, and behavioral traits such as voice, gait, etc.

In a world where technology has advantages and disadvantages, terrorists as well as state agents use several techniques to penetrate the system and hack the database. Although biometrics are generally more secure, they are not foolproof. Terrorist hackers spoof biometric data using various techniques such as downloading or printing a person's photo, using a fake silicone fingerprint or a 3D mask. Such attacks are called presentation attacks.

Additionally, smartphone fingerprint scanners often rely on partial matches. Researchers have discovered that it is possible to create “master fingerprints” that match the partial fingerprints of many people and can thus provide access to a large number of user accounts.

In addition to being hackable, biometric systems can also sometimes fail to recognize a valid user: someone might be wearing different makeup or new glasses, or a user's voice might be different when they are sick or he just woke up. There are some serious ethical concerns surrounding many forms of biometrics. One of them involves bias. Facial recognition systems may not recognize persons of color or non-cisgender people as accurately.

Moreover, many biometric systems have been trained primarily using white or white male photos. This incorporates in them an inherent bias that results in difficulty recognizing women and people of color.

Summary

In this research literature, the objective was to establish a baseline on the composition of intelligence with its challenges, the scale of terrorism, and the means to combat terrorism. It was also about understanding how intelligent counterterrorism agents and enemies (terrorists) used specific techniques that could affect operations inside or outside the country. A literature review on collection methods with OSINT, data breaches, and biometrics was conducted. These sections explored how adversaries use various TTPs to identify, target, and expose authorized personnel and intelligence operations.

The intelligence cycle has been invoked to explain the distinction between information and intelligence, which is further a process of transforming raw information into finished intelligence and enabling consumers to make decisions and take action.

The main weakness of the agencies of the countries allied to the United States was mentioned. Thus, the literature review focused on the use mainly of news articles and special publications regarding terrorism; intelligence, counterterrorism, and data breaches with biometric identification methods that could compromise intelligence operations.

CHAPTER THREE
METHODOLOGY

Introduction

A well-defined methodology will be employed to clarify the findings for the readers. Methodology refers to the underlying reasoning behind the research approach and the perspective through which the analysis is conducted. It outlines the general research strategy that guides how the research will be conducted, and serves as an introduction to the Philosophy of Methodology (Howell, 2013).

This thesis aims to explore the relationship between intelligence and protection against terrorism. To achieve this, the thesis has utilized two distinct powerful combinations of research methods to facilitate a comprehensive investigation. By implementing the qualitative research method, this study meticulously interprets and analyzes historical facts to uncover new insights. Additionally, the exploratory methodology aims to identify practical solutions to the complex research question at hand. The study will investigate how intelligence has evolved in terms of its ability to safeguard nations against terrorist threats. Exploratory research was conducted to examine research questions that have not been studied in depth. In this case, the subject of the research is counterterrorism, which is "undertheorized and understudied," as Byman and Daniel (2007) stated. The study will examine changes over time in the ability of intelligence to protect nations against terrorism. The study is based on a literature analysis of intelligence theory, terrorism, and counterterrorism. The subject matter is not easily understood at first glance. Throughout this study, the discovery of information on biometrics, data breaches, open sources, and the intelligence cycle will occur gradually. To establish the framework for this study, we will conduct a systematic review of the case studies. This chapter will review the US intelligence community which, despite its robust intelligence agencies focused on state actors, continues to face the threat posed by elusive terrorists who use unconventional methods relatively unsophisticated and cause casualties. This technique used by terrorists constitutes a more complex intelligence task (Zegart, A. B., 2005).

This chapter will discuss the importance and role of current intelligence agencies and the intelligence cycle in the context of global security within intelligence. Due to their significance as global security topics, intelligence, terrorism, and counterterrorism require critical examination of issues related to surveillance, control, and effectiveness. The analytical approach for this research comprises two crucial components: the selection method and the type of significant cases. The crucial case selection method defines cases that are critical to a broader concept or set of theories. A crucial case is chosen when it is a question of defining, or at least illustrating, a concept or a theoretical result, however, the type of crucial case reveals an unexpected result concerning the causal inference studied (Gerring, John, 2001).

For this reason, this study chose several categories of case studies: Category I - Intelligence, counter-terrorism, and counter-intelligence services of the United Kingdom, the United States, France, and the Democratic Republic of Congo. Category II: - Data breaches including open-source intelligence and the Robin Sage affair. Category III: - Intelligence life cycle category, including planning and direction - intelligence gathering - intelligence processing - intelligence analysis/production - intelligence dissemination - information feedback. British intelligence services are an old model that most countries, and even the United States, have copied. To this long history of maintaining order has been added a long history of the development of domestic intelligence. In both cases, foreign intelligence and domestic intelligence can provide relevant examples from the perspective of what works well and what does not. The cases of the United Kingdom and the United States will enable the development of a grounded theory of domestic intelligence. The Grounded Theory approach will be used in this intelligence-related study to collect and analyze data. A conceptual framework categorizing themes and item categories will be developed based on empirical evidence linked to previous studies which will ultimately reflect the findings of the field. The most fundamental elements of this conceptual framework will be six components categorized into themes: Planning and direction - intelligence gathering - intelligence processing - intelligence analysis/production - intelligence dissemination - information feedback.

The research design and case studies will be used to show how intelligence operations and their personnel will continue to be affected by foreign government adversaries using OSINT and information from data breaches in conjunction with biometric screening technology by foreign government adversaries and terrorists. The danger of OSINT is that it remains a vulnerable multifactorial methodology (qualitative, quantitative) that allows collecting, analyzing, and making decisions on data accessible in publicly available sources for use in an intelligence context. Its vulnerability heightens suspicions of abuse by enemies of the United States, willing to steal intelligence data and counterterrorism information from the United States through authorized personnel supporting the foreign intelligence mission (Call 2011).

Organizational leadership in the context of an internal security framework will be respected and strengthened to the extent that there is a fair and open system of information sharing, with appropriate legal and procedural constraints, which are key ingredients for success. This information-sharing system makes it possible to resolve key issues before achieving a true synergy of the intelligence structure in the domestic context, which takes into account the need for well-defined authorities, responsibilities, and missions as clearly as possible (Hobart, P. M., 2008)

Surveillance, effective control of terrorism

The surveillance method used by terrorists is strategically simple because they can use aggressive surveillance techniques. These threats can range from false telephone threats to approaching security checkpoints to ask for directions or an "innocent" attempt to smuggle non-lethal contraband through checkpoints. At the checkpoint, terrorists aim to study weak points or failures in surveillance. To better combat international terrorism, surveillance, and intelligence agents should lead the fight against terrorism by relying on a surveillance network in collaboration with other countries very committed to the fight against terrorism.

Research Design and Methodology

Case studies will be used in this study to show common behaviors or characteristics. Mintzberg, McHugh (1985), Eisenhardt, K. M. (1989) Sutton & Callahan (1985) use case study as a research strategy to focus on understanding of the dynamics present in a unique context. This strategy combines data collection like archives, interviews, observations. Sutton and Callahan (1987), rely on qualitative data in their study of bankruptcy in Silicon Valley, unlike Mintzberg and McHugh (1985).

Finally, case studies are used to achieve various goals: providing a description (Kidder 1982), a test theory (Pinfield 1986; Anderson 1983) or generating a theory (e.g., Gersick 1988; Harris & Sutton 1986).

The results that will emerge from this study of the cases will demonstrate the relevance of the subjects raised and the action that will result after studying the needs. Using analyses and information on the subjects raised in this study, light will be shed on the impact of intelligence operations and counterterrorism.

Research Design

The information used in this study comes from analyzed information found through open source research, and which only contains data from reputable academic publications and government reports. The primary objective of choosing this methodology in addition to direct investigation is the use of case study methodologies to collect information in open-source intelligence of operational TTPs, data breaches of PII of the US cleared personnel and biometrics as a means for adversaries to expose US cleared personnel and the intelligence operations they support. The appearance of new gadgets or the theft of information either through biometric or other operating methods, become a phenomenon to be observed and analyzed. From this study, phenomenological reflection may refer to methods of analyzing empirical data and, more broadly, to a guiding philosophy that can be used to facilitate reflection and help uncover hypotheses to answer this research question study.

Selection of Cases

To better understand the case studies, it is necessary to shed light on the selected cases. There are three categories of case studies and several specific case studies, which make up all of the case studies in this research work. The three categories and case studies are Intelligence Services, Anti-terrorism Services, and Counter-espionage Services. The specific case studies are linked to the intelligence and counter-espionage category of the selected countries, which are the United Kingdom, the United States, France, and the Democratic Republic of Congo.

The second category is Internet use. Specific case studies focus on data breaches, open-source intelligence, and the Robin Sage affair.

The third category is the Intelligence Life Cycle category, which includes specific cases such as planning and directing, intelligence collection, intelligence processing, intelligence analysis/production, intelligence dissemination, and feedback.

Since this study will use several categories of case studies, including:

Category I: **-** Intelligence services, counter-terrorism services, and counter-intelligence services of *a) the United Kingdom, b) the United States, c) France, and d) the Democratic Republic of Congo.*

Category II: - Internet used of a) Data breaches b) open-source intelligence and c) the Robin Sage affair.

Category III: - Intelligence life cycle category, including: *a) planning and direction*
b) Intelligence gathering – c) intelligence processing – d) intelligence analysis/production –
e) Intelligence dissemination – f) information feedback,

It is important to use the models that researchers often use when dealing with multiple cases in academic practice. A multi-case study is a research method that involves selecting and analyzing two or more cases that share certain common characteristics but differ in some aspects. The cases can be chosen based on criteria such as typicality, diversity, replication, contrast, or theoretical testing. In a multiple case study, researchers repeat the study process between cases to study the same phenomena. The difference between single and multiple case studies lies in the research design, which falls under the same methodological framework. To write a multiple-case study, a summary of individual cases should be reported, and researchers need to draw cross-case conclusions and form a cross-case report (Yin, 2017).

With evidence from multiple cases, researchers may have generalizable findings and develop theories (Lewis-Beck, Bryman & Liao, 2003)

Emphasis should be placed on the importance of within-case analysis. Therefore, it is advisable to choose one of the best-known and often-used models by Alexander George and Andrew Bennett (2004).

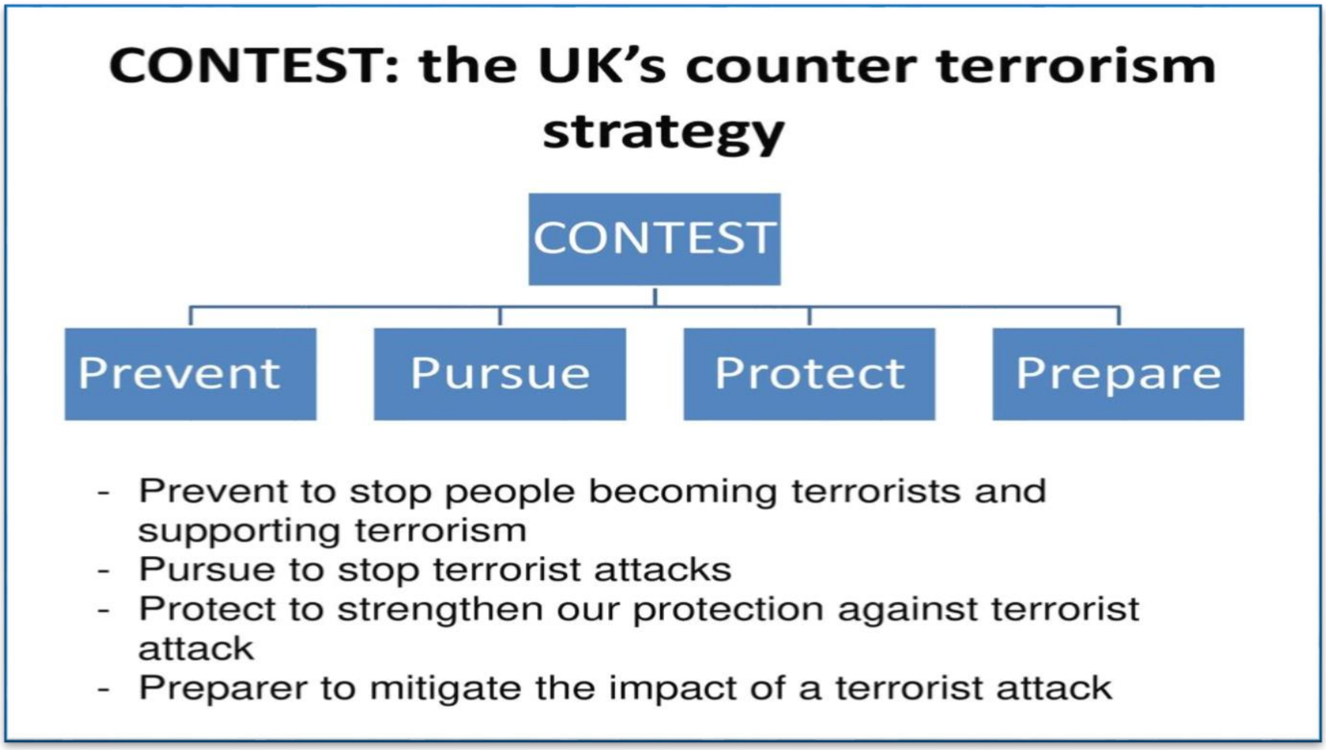
Category I of case studies: Counterterrorism Structures.

The United Kingdom's counterterrorism structures: This work will examine the UK's counterterrorism structure which is called Counterterrorism Terrorism Strategies (CONTEST) with the mission of countering terrorism. How well the United Kingdom is coping with the terrorist threats. Is the counterterrorism structure consistent? CONTEST is recognized as one of the most successful strategies in the world, with an intentional focus on community support and what is now called “prevention” (or counter-extremism) measures. CONTEST has four pillars in its program: *Prevent, Protect, Prosecute, and Prepare.*

CONTEST has a long history of countering terrorism, particularly concerning nationalist terrorism originating from Northern Ireland and the Irish Republican Army (IRA) in the 1970s. Just before the events of 9/11, the Terrorism Act 2000 was passed and was the first piece of legislation to recognize the changing landscape of terrorism, particularly the rise of Islamist terrorism, in the UK and around the world.

The threat of terrorism, globally and in the UK, is significantly higher than in 2011. The UK faces several and persistent terrorist threats. The increased threat is primarily due to the rise of ISIS and the creation of its sectarian “caliphate,” combined with the threat from Al-Qaeda. ISIS and al-Qaeda exploit the internet to promote distorted alternative narratives, urging extremists within communities to overthrow the Western way of life through, brutal violence.

<u>CONTEST Strategic Structure</u>



CONTEST: the UK's counter terrorism strategy

CONTEST

Prevent

Pursue

Protect

Prepare

- Prevent to stop people becoming terrorists and supporting terrorism
- Pursue to stop terrorist attacks
- Protect to strengthen our protection against terrorist attack
- Preparer to mitigate the impact of a terrorist attack

Fig.2: The referral process into Channel

Source: GOV.UK: Counter-terrorism strategy (CONTEST)

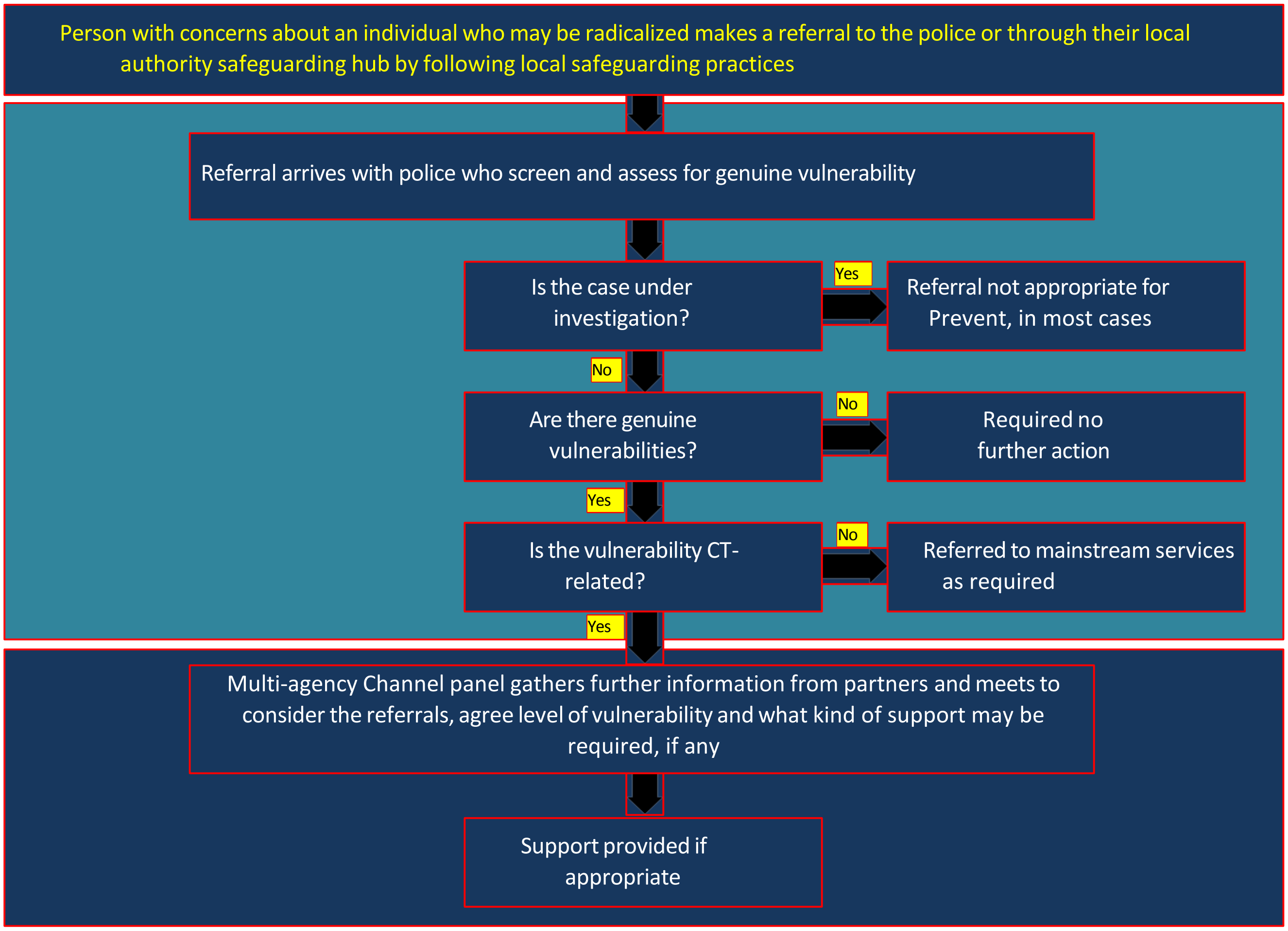
In conclusion, a change under a new approach must have radically altered national investigative capabilities through the operational improvement experience of MI5 and CT Policing who used the policing approach. A new anti-terrorism legislation which ensures that police and prosecutors have the necessary powers to enable intervention at an earlier stage of investigations, leading to prosecutions for terrorist offenses, supported by longer prison sentences and more effective management of the strict control of terrorist activities of offenders even after their release.

With the creation of the CONTEST which specifically deals with terrorism with four identified and distinct pillars, terrorism will be defeated. The advantage of the CONTEST Structure is that the specialized services do not confuse their task and their missions with that of the foreign police or the criminal police, but this structure has its specialized agents. In doing so, the structure will be able to collect information on the first pillar which is "Prevention".

CONTEST is a well-organized and comprehensive risk reduction framework that coordinates well between government departments and agencies, as well as international and private sector partners, to achieve its objectives. The CONTEST framework includes the work streams Prevent, Prosecute, Protect, and Prepare remains an effective way of organizing anti-terrorism actions.

The UK's counter-terrorism system has had to improve its system of sharing information more widely and support more local interventions with individuals in communities who are being manipulated or instigated to commit or support acts of terrorism. Abroad, the UK remains committed to the Global Coalition's campaign against Daesh, aimed at stripping it of territorial control, further degrading its media capabilities, and disrupting key leaders and networks. The UK has led international efforts to improve the fight against terrorism globally, with campaigns led by ministers on aviation security and preventing terrorist use of the internet. Terrorism also threatens UK businesses operating globally and the UK's wider interests in stability, prosperity, governance, human rights, and development.

Processing into Channel


Person with concerns about an individual who may be radicalized makes a referral to the police or through their local authority safeguarding hub by following local safeguarding practices
Referral arrives with police who screen and assess for genuine vulnerability
Is the case under investigation?
Yes
Referral not appropriate for Prevent, in most cases
No
Are there genuine vulnerabilities?
No
Required no further action
Yes
Is the vulnerability CT-related?
No
Referred to mainstream services as required
Yes
Multi-agency Channel panel gathers further information from partners and meets to consider the referrals, agree level of vulnerability and what kind of support may be required, if any
Support provided if appropriate

.Fig 3: Process steps

Channel is a program that "focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. The program uses a multi-agency approach to protect vulnerable people by: identifying individuals at risk; assessing the nature and extent of that risk; and developing the most appropriate support plan for the individuals concerned

The United States counterterrorism structures

Due to the significance of the terrorist threat following the September 11 attacks, how the United States responded to the terrorist threat, the effectiveness of the measures taken, and the timeliness of those measures have been precipitated. Recognized values of personal liberty and liberty have been challenged in public and political debates. Terrorism and Intelligence covered issues relevant to all domestic and foreign intelligence efforts, rather than just domestic intelligence. Questions remain about whether the United States has adequate organizational and technical tools to protect the nation or whether it needs an additional dedicated intelligence agency.

Terrorism remains a priority for Americans in their fight against terrorism domestically. The big concern is whether Americans' prevention efforts are commensurate with the threat facing their countries. One element of this debate is whether the United States should create a domestic intelligence agency with a foreign branch dedicated to fighting terrorism. Case studies from other countries such as France, the Democratic Republic of Congo, and the United Kingdom provide common lessons and themes that can help policymakers make decisions.

This study reveals that: Most countries separate the agency responsible for national intelligence collection from any powers of arrest and detention, ensuring effective collection, analysis, and operations. Each country has instituted some measure of external oversight over its national intelligence agency. Liaison with other international, foreign, state, and local agencies ensures better information sharing. The boundary between national and international intelligence activities has become permeable and on the Internet, with new technologies, we are also witnessing information theft and collection abuses.

How to deal with the threat of "lone wolf" terrorism

The draconian measures taken by the United States to combat terrorism have undermined the modus operandi of terrorists, some of whom have immigrated to countries where there is a weak counterterrorism structure such as in Africa and the Middle East and there are others who radicalized individually to operate alone as "Lone Wolf". The challenge for the Americans is how to end terrorism and with what form of structure to put in place.

Identifying, targeting, and stopping a lone wolf is very difficult. They are solitary actors, whose intentions are difficult to discern because they avoid contact with others. When activists operate in a cell of several people, there is a greater chance that one of them will become frightened and reveal the plot to authorities, or that law enforcement and intelligence services will intercept communications between the conspirators, or that law enforcement authorities will be able to introduce an informant into the group" (Artiga, Vic, 2010).

It is very difficult to predict from what disenfranchised, alienated, or frustrated environment they come. They have varied backgrounds and a wide spectrum of ideologies and motivations. Third, it is extremely difficult to differentiate between extremists who intend to carry out attacks and those who simply express radical beliefs or issue empty threats (Clemons, Steve, 2010).

It is extremely difficult to identify potential lone wolves before they attack, even with the help of the most sophisticated intelligence collection tools. With such a vast universe of potential suspects, it's like picking up haystacks to find a needle. Challenges of the Lone Wolf Fortunately, there are also some operational constraints for the lone wolf, when executing a “successful” attack. Like all terrorists, they are bothered by the cycle of terrorist attacks. And since they work alone, they must carry out each step of the cycle themselves.

This means they are vulnerable to detection at several different times when planning their attacks, the most critical being the surveillance phase of the operation (Hewitt, Christopher; 2003).

With the apparent increase in lone-wolf Islamist terrorism, new questions arise, about the development of the concept of "leaderless jihad", the role of the Internet, and the possible impact of Islamist lone-wolf attacks on societies in general and Muslim communities and Islamist subgroups in particular. Certainly, there is an effect of contamination or inspiration of solitary Islamist terrorism which spreads because of the link between the success of anti-terrorism measures against Islamist terrorist networks and the rise of propaganda in favor of solitary action without receiving instructions.

Lone Wolf as a Tactic

The Lone Wolf is not always active; he falls asleep and wakes up depending on the circumstances. The tactics of the fighters of this type of terrorist indicate that the fighters may be members of a network, but this network is not a hierarchical organization in the classic sense of the term (Artiga, Vic, 2010).

The terms "targeted society" and "self-activation" imply that the lone wolf acts rationally and that his actions are directed against that society or parts of it. These acts are politically or religiously motivated and aim to influence public opinion or political decision-making.

Strengthening of Lone Wolf in the USA

The increase in lone-wolf terrorism in the United States over the past three decades can be explained in part by the adoption and spread of this method by and among right-wing extremists (Hamm, Mark, 2002).

In the late 1990s, the white supremacists mentioned above, Tom Metzger and Alex Curtis, explicitly encouraged their fellow extremists to act alone by committing violent crimes (COT, ed, 2007).

According to Beam Louis (1992), a few years earlier, white supremacist Louis Beam, a former member of the Ku Klux Klan and the Aryan Nations, had popularized the strategy of leaderless resistance. His vision was that all individuals and groups operate independently of one another and never report to a central headquarters or single leader for direction or instruction.

Office of the Director of National Intelligence (ODNI)

The Office of the Director of National Intelligence (ODNI) integrates the intelligence collection and analysis functions performed within the Intelligence Community to provide intelligence to policymakers and oversee Intelligence Community (IC) integration; provides information, builds capacity, and invests in the future. The ODNI is composed of officers from across the IC and is organized into directorates, centers, and oversight offices that support the DNI's role as head of the IC and manager of the National Intelligence Program (NIP). In their roles as functional National Intelligence Officers (NIMs), the National Counterterrorism Center (NCTC), the National Counter proliferation and Biosecurity Center (NCBC), the National Counterintelligence and Security Center (NCSC), the Cyber Threat Intelligence Integration Center and the Ministry of Foreign Affairs, all these agencies contribute to the intelligence integration mission. The U.S. intelligence community is a large and complex structure, organized and managed under a multitude of laws, executive orders, policies, and directives. The purpose of the following discussion is to provide an overall, albeit simplistic, picture of the Community and how it works, and to serve as a guide for those unfamiliar with the subject.

The essential role of intelligence is not difficult to understand. This is about providing timely and relevant information to U.S. policymakers and warfighters. Accomplishing this mission involves tasking, collecting, processing, analyzing, and disseminating intelligence, commonly referred to as the "intelligence cycle."

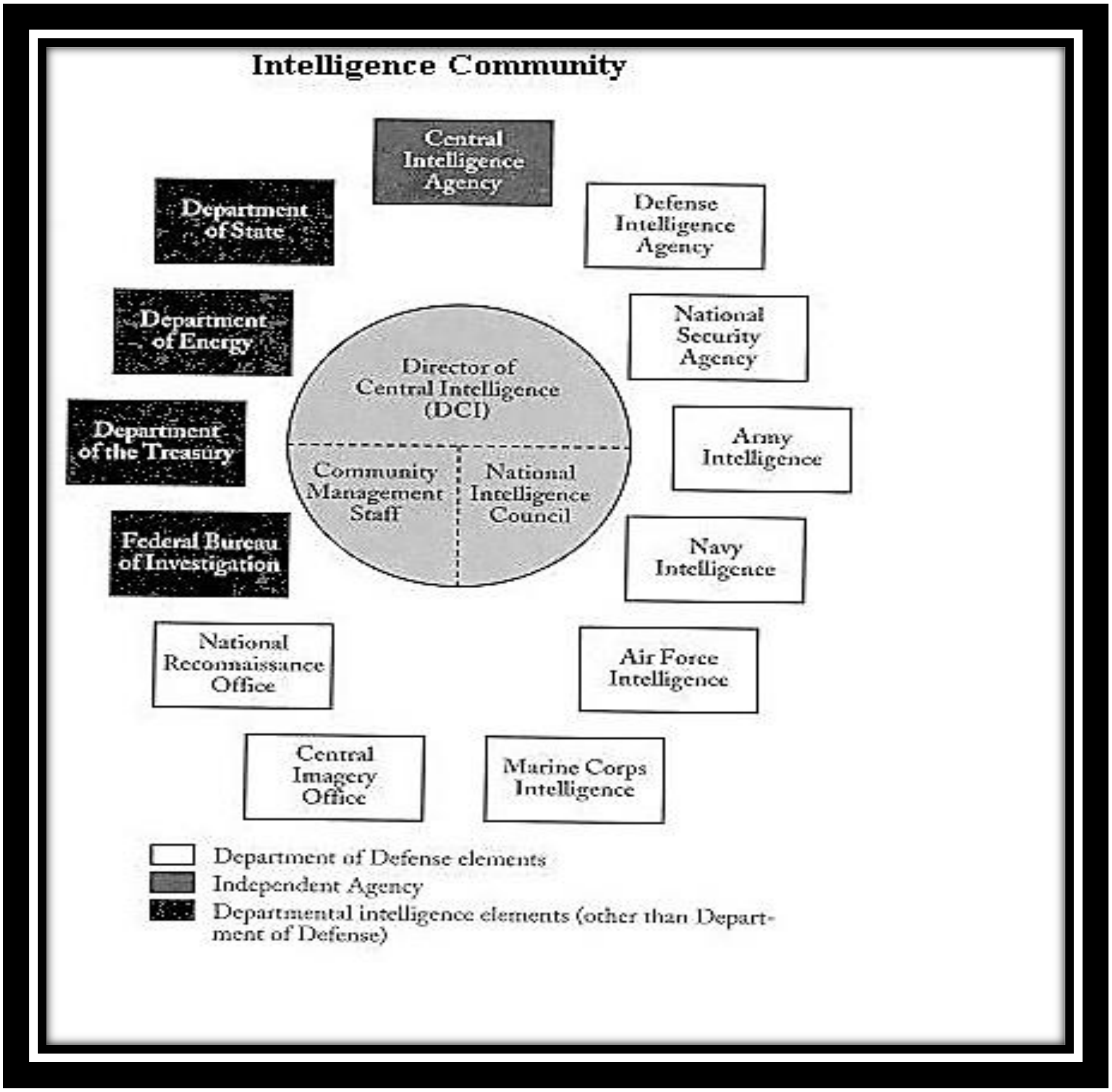

Intelligence Community
Central Intelligence Agency
Department of State
Defense Intelligence Agency
Department of Energy
National Security Agency
Director of Central Intelligence (DCI)
Department of the Treasury
Army Intelligence
Community Management Staff
National Intelligence Council
Federal Bureau of Investigation
Navy Intelligence
National Reconnaissance Office
Air Force Intelligence
Central Imagery Office
Marine Corps Intelligence
Department of Defense elements
Independent Agency
Departmental intelligence elements (other than Depart-ment of Defense)

Fig. 4 Intelligence Community

The specialized structure of American counterterrorism

The National Counterterrorism Center (NCTC) is a US structure that was created after 9/11 to reorganize and restructure the Intelligence Community (IC) to protect and secure the country from terrorist attacks. The NCTC has four main directorates: Intelligence, Terrorist Identities, Operations Support, and Strategic Operational Planning, as well as nine offices that provide critical functions, including intelligence management and innovative data acquisition.

The mission of the NCTC is to lead the nation's efforts to protect the United States from terrorism by integrating, analyzing, and sharing information to drive whole-of-government action and achieve national counterterrorism goals. The center provides a unique environment to leverage the collective knowledge and formidable capabilities of the U.S. government to identify and counter the terrorist threat facing the country (Bennie G. Thompson, 2006 p.6).

The NCTC reports to the Office of the Director of National Intelligence (ODNI). The director of the NCTC is appointed by the President and confirmed by the Senate. The D/NCTC reports to the Director of National Intelligence (DNI) as the national intelligence officer for counterterrorism and serves as the principal advisor to the DNI for CT-related intelligence operations. The D/NCTC reports directly to the President for CT strategic operational planning activities. The NCTC includes several employees from different organizations, including the Central Intelligence Agency, the Department of Justice/Federal Bureau of Investigation, Departments of State, Defense, and Homeland Security, etc

NCTC Organizational Structure

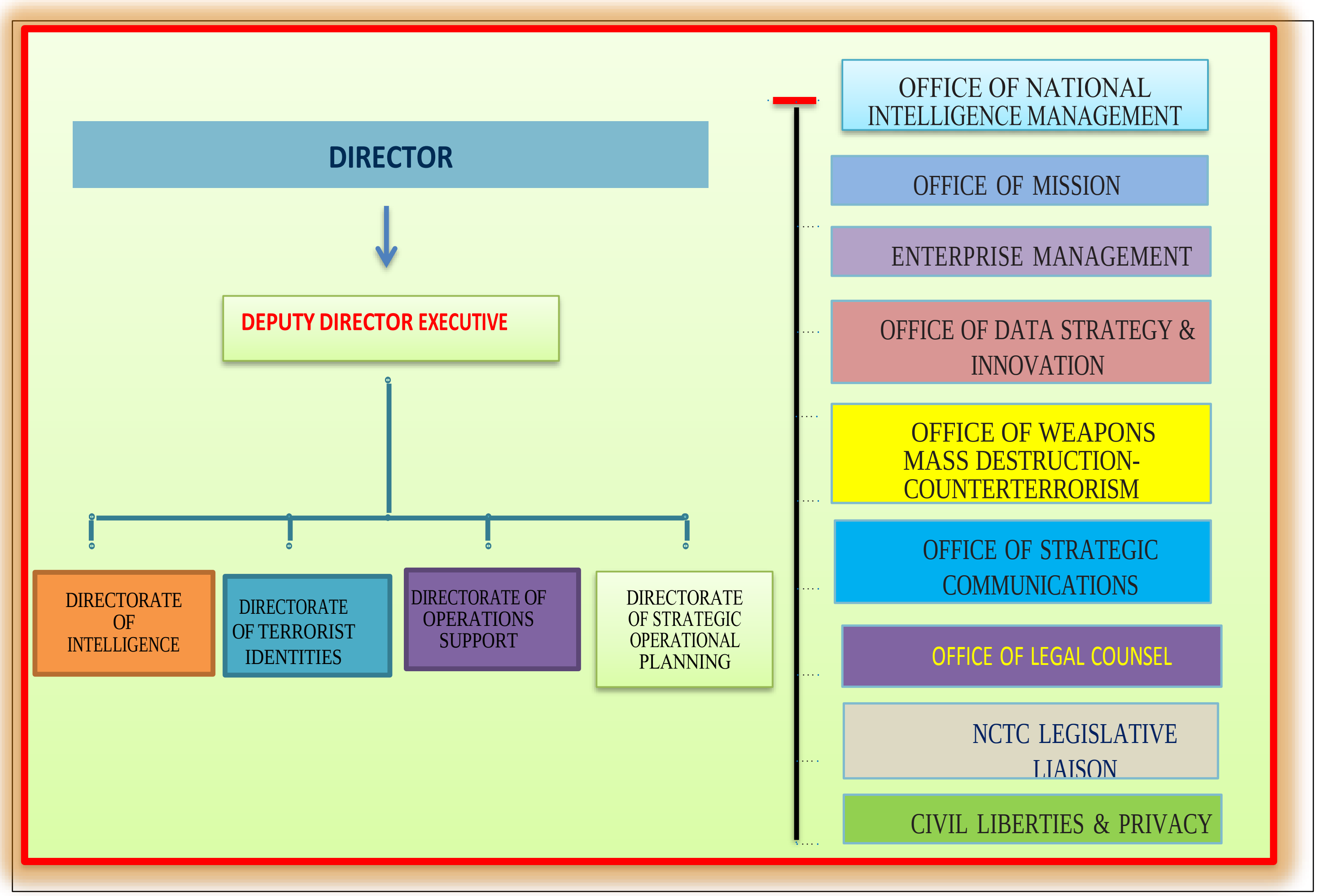

DIRECTOR
DEPUTY DIRECTOR EXECUTIVE
DIRECTORATE OF INTELLIGENCE
DIRECTORATE OF TERRORIST IDENTITIES
DIRECTORATE OF OPERATIONS SUPPORT
DIRECTORATE OF STRATEGIC OPERATIONAL PLANNING
OFFICE OF NATIONAL INTELLIGENCE MANAGEMENT
OFFICE OF MISSION
ENTERPRISE MANAGEMENT
OFFICE OF DATA STRATEGY & INNOVATION
OFFICE OF WEAPONS MASS DESTRUCTION-COUNTERTERRORISM
OFFICE OF STRATEGIC COMMUNICATIONS
OFFICE OF LEGAL COUNSEL
NCTC LEGISLATIVE LIAISON
CIVIL LIBERTIES & PRIVACY

Fig 5: NCTC Organizational Structure

NCTC has set a new standard for information sharing and analysis by combining unprecedented access and data integration with a diverse workforce made up of experts from across the Federal government and state and local first responders.

NCTC's Key Mission Areas

NCTC performs five key missions in support of our Nation's CT efforts. The Center is authorized to access all terrorism-related information held by the USG.

Mission Area I: Threat Analysis: NCTC serves as the primary organization in the USG for analyzing and integrating all intelligence possessed or acquired by the USG of terrorism and CT except intelligence pertaining exclusively to domestic terrorism.

Mission Area II: Information Sharing: In addition to fulfilling its own analytic and planning responsibilities, NCTC ensures that other agencies with CT missions have access to and receive intelligence needed to accomplish assigned activities.

Mission Area III: Identity Management: NCTC has the statutory responsibility to serve as the central and shared knowledge bank on known and suspected terrorists, as well as their goals, strategies, capabilities, and networks of contacts and support.

Mission Area IV: Strategic Operational Planning: NCTC also has the statutory responsibility to conduct strategic operational planning for CT activities across the USG, integrating all instruments of national power—diplomatic, informational, military, and economic within and among the agencies. NCTC ensures unity of effort for planning include broad strategic plans as well as specific action plans to maximize coordination on key issues

Mission Area V: National Intelligence Management: NCTC's role requires integrating the CT mission across intelligence functions, disciplines, and activities to achieve unity of effort and effect. NCTC leads U.S. IC efforts to optimize CT community performance and capabilities, and advocates on behalf of the CT community to ensure the U.S. IC is postured to support national strategy and policy objectives.

Conclusion

Through these unique authorities, NCTC personnel can effectively bridge the gap between foreign and domestic intelligence, allowing the Center to take a whole-of-government approach in each mission area. This action fails to accommodate overall counterterrorism protection in U.S. allied countries, which the U.S. should sincerely support given that terrorists establishing bases in foreign countries aim to return in force and attack the U.S. and its allies

The France's Counterterrorism structures

Vigipirate in France: France has unfortunately experienced multiple terrorist attacks, which has led to the Vigipirate plan being elevated to the "Emergency Attack" level. The Vigipirate plan is a comprehensive global surveillance, prevention, and protection strategy that encompasses all sectors of activity in France. It involves all French ministries and the entire population and is intended to monitor terrorism rather than combat it directly.

The Armed Islamic Group (GIA), also known as al-Jamm'ah al-Islamiah al-Musallah or the Groiipe Islamique Arme, is the primary group responsible for directing the terrorists on French soil. The Vigipirate plan has proved successful in reducing terrorist attacks due to the experienced anti-terrorist apparatus in place. However, the structure needs to be adjusted to allow the services dealing with other types of crimes to be separated from the counterterrorism.

History of terrorist violence in France**:** Starting in the mid-1970s, France and other European countries faced separatist or left-wing terrorist threats. From the beginning of the 1990s, Islamist extremists had to recruit young people in the poor suburbs of France and radicalize several of them to undertake terrorist operations. The Islamist terrorist threat increased when the Algerian government overturned the victory of the Islamic Salvation Front (FIS), Algeria's largest Islamic opposition party of Algeria's legislative elections in 1991.

The French government's view on combating terrorism: In response to attacks from the GIA, French intelligence services took swift action to dismantle the group's networks. This caused the GIA to shift its logistics, finances, and propaganda efforts to other European countries, particularly the United Kingdom. Eventually, the group was forced to move to African countries with weaker surveillance. Over time, the GIA's influence waned due to internal tensions among its core members over the use of extreme violence against civilians, including fellow Muslims, as well as French counterterrorism efforts.

However, the French anti-terrorism apparatus has a weakness in that it treats anti-terrorism investigations in the same way as criminal investigations. This approach delegitimizes the terrorists' "cause," as they are treated like any other dangerous criminal. The French government believes that special jurisdiction for enemy combatants at Guantanamo Bay is counterproductive because it elevates terrorists to a higher level of importance, thereby reinforcing their narrative. These measures do not put pressure on terrorists.

France views the terrorist threat differently than the United States. While France recognizes Islamist terrorism as a major threat, it does not view terrorist actions as an "act of war" against France or the West as a whole. This perspective is not shared by other US allies.

***French counterterrorism tactic*:** France has a strategic plan in place to combat terrorist groups. French intelligence agencies prioritize international collaboration, human sources, and the training of counterterrorism agents. They address the psychological aspect of the mission by following a strict three-level approach that combines conformity, coherence, and convergence. This approach means that for the effectiveness, the fight against terrorism must be inventive and flexible in respect of the law. Renouncing democratic principles to pursue an anti-terrorism mission will aid terrorists in spreading their ideology and reinforcing their "martyr" narrative.

Another tactic employed by French law enforcement to prevent terrorist attacks is to "incite" one or more suspects to break the law, often by using undercover agents. This is permitted in the French legal system if the goal is to prevent a more dangerous or imminent offense. Intelligence services use the same tactics to trace a network. These special clauses only apply to cases related to pimping, narcotics, and threats to state security, including terrorism.

Conclusion

France has faced terrorist threats for decades. There is no independent authority responsible for controlling French intelligence or counter-terrorism agencies. However, it has a well-established anti-terrorism apparatus that benefits from several laws with no real equivalent in the United States, from the possibility of arresting any person linked, even remotely, to a “criminal”, up to detention in a more secret place.

The Democratic Republic of Congo’s Counterterrorism structures

ISIS–Democratic Republic of Congo (ISIS-DRC), also called ISIS–Central Africa and locally known as the Allied Democratic Forces (ADF), is one of the deadliest militant groups in eastern Congo. The group began as an antigovernment insurgency in Uganda and was publicly recognized by ISIS leaders in Syria as an ISIS branch in 2019. ISIS-DRC follows ISIS’s strict interpretation of Islamic law and aims to extend ISIS’s self-proclaimed caliphate into central Africa.

Operating Areas*:* The terrorists are mainly found in the North Kivu and Ituri provinces of the DRC, also carrying out attacks in Uganda and advancing towards the entire Great Lakes sub-region. There are over 130 active armed groups in eastern DRC. Armed conflict has caused widespread civilian displacement and deaths. Conflict between local armed groups and government forces is ongoing. It's a more serious threat in eastern and Northern provinces.

Tactics and Targets**:** ISIS-DRC has a history of indiscriminate killings, ambushes, and kidnappings against Congolese citizens, regional military forces, and UN personnel in the DRC and Uganda. Its attacks killed approximately 4,000 civilians from 2014 to 2020. In 2021, the branch began using IEDs to conduct attacks in Uganda.

Foreign Terrorist Group Designation

The US State Department designated ISIS-DRC as a foreign terrorist organization in March 2021 and designated the branch's leader, Seka Musa Baluku, a specially designated global terrorist at the same time. In 2014, the ADF—ISIS-DRC's predecessor group was sanctioned by the US Treasury Department and the UN under the UN Security Council's DRC sanctions regime for violence and atrocities. The Islamic State group has been funding the Allied Democratic Forces for several years, leading to an escalation of brutality. A United Nations panel of experts' report outlines the latest development in relations between one of Central Africa's deadliest terrorist groups and the Islamic State group, which is seeking to expand its footprint on the continent after losing on the ground in the Middle East.

The Allied Democratic Forces, based in the Democratic Republic of Congo (DRC), are accused of attacking a dormitory in western Uganda in mid-June, killing 41 people. The attackers set the building on fire, fired wildly, then used machetes to kill the survivors. It was the deadliest attack in Uganda in more than a decade.

Since 2017, the Kivu Security Tracker has reported 999 incidents involving the Allied Democratic Forces in the eastern provinces of the DRC bordering Uganda and Rwanda. As of October 2020, the Islamic State group claimed responsibility for 72 attacks in the DRC, 65% of which were directly linked to verified Allied Democratic Forces attacks.

A large number of attacks took place across the border in Uganda's Kasese province, where the school shooting occurred in June. The UN report also reveals links between the Allied Democratic Forces and the Ahlu Sunnah Wal Jama'a militia in Mozambique, which has also declared allegiance to the Islamic State. With official Islamic State affiliates and pro-Islamic State groups scattered across Africa, the potential for cross-border collaboration and the movement of greater numbers of foreign fighters could threaten regional stability.

These terrorists based in the Central African region (DRC) have specialized in money laundering operations, equipping themselves and training other fighters to attack the United States and allied countries soon. Global counterterrorism measures must be taken by the U.S. to protect its homeland, protect its allies, and protect the international community as a whole.

Notable Terrorist Attacks

Date of Events	**Location**	**Events**
25 DEC. 2021	**Beni, DRC.**	*An ISIS-DRC suicide bomber detonates a vest at a bar, killing seven people and wounding about a dozen others, including two DRC Government officials*
16 NOV. 2021	**Kampala, Uganda**	*ISIS-DRC operatives detonated explosives in front of a police station and near the Ugandan Parliament building, killing at least seven people, including the bombers, and injuring dozens, marking the first time ISIS has successfully conducted a suicide attack in Uganda.*
MAY 2021	**Beni, DRC**	*ISIS-DRC operatives assassinate two prominent imams who had spoken out against ISIS*
OCT. 2020	**Beni, DRC**	*ISIS-DRC members raid the Kangbayi central prison, releasing more than 1,000 prisoners.*
13 MAY 2020	**Beni, DRC**	*ISIS-DRC operatives attack three villages, killing nearly 30 people*

Table of Notable Terrorist Attacks

(Sources: Director of National Intelligence (.gov) ISIS–Democratic Republic of Congo (ISIS-DRC)

Intelligence services and Counterterrorism system of the DRC

The Democratic Republic of Congo (DRC) has two security services, namely the National Intelligence Agency (ANR) and the Military Detection of Anti-Interior Activities (DEMIAP). These agencies are responsible for maintaining the internal and external security of the state. The President of the Republic has the authority over both agencies, and they are subject to other missions conferred by specific texts. While one of the agencies serves the military, the other serves civil society.

Apparatus for combating Congolese Terrorism - DRC

The Democratic Republic of Congo is facing a grave issue of terrorism and crime, yet the government has failed to take any significant measures to combat it. Even though the DRC is an ally of the United States, there has been no assistance provided by them to fight against domestic terrorist groups such as Kuluna.

It is high time for the government to take immediate action and reduce the threat of these groups that are multiplying rapidly in the country. The government should focus on developing an integrated counter-terrorism approach by winning the support of the local population, and by working together with governments, regional organizations, and the international community to combat terrorism and crime in the East of the Republic.

African countries, including the Democratic Republic of Congo, should work on creating tools to collect, analyze, process, and share information about terrorism-related activities taking place in Africa. These countries are important allies of the United States of America, and hence, it is incumbent upon the US to intervene and aid in finding lasting solutions for combating terrorism, promoting good governance, and fighting against money laundering and drug trafficking.

Category II of case studies

First case study: Data Breaches

The second category topic will be data breaches including Open-source intelligence and the Robin Sage case. Data breaches which are the primary modus operandi used by adversaries to compile sensitive data on authorized personnel. The enemies are The enemies are multifaceted they can be terrorists or drug traffickers who operate with terrorists and launder money, but also "great powers countries" like the United States, China, Russia and Great Britain, taken as examples, which would seek to attack computer installations from another country either to steal information or to destroy data. This case study will review the Information stolen or otherwise obtained from the websites of OPM, United Airlines, Anthem Insurance, and Ashley Madison (Botha 2015 and 2016).

From the unprotected websites, information from OPM, United Airlines, Anthem Insurance, and Ashley Madison was obtained and evaluated to determine that, the information combined, creates a sort of destructive counterintelligence profile of the US cleared personnel who support, both inside and outside the borders, several intelligence operations. A data breach occurs when Personally Identifiable Information (PII) has been maliciously lost or stolen and is therefore at risk of exposure (Romanosky, S., Sharp, R., & Acquisti, A., 2010).

The use of Facebook by the Chinese government demonstrates how Chinese people will compile and analyze the information gathered to determine how certain US cleared personnel will be targeted and what their past travel habits have been. They will also go further to determine the type of operations they could support abroad if necessary and how they may be likely to be identified at border crossings by biometric identification procedures.

Evaluating how biometric technology affects intelligence operations by targeting the US cleared personnel who support them was the final subject method researched. Two high-profile case studies were evaluated to demonstrate how biometrics, with the help of OSINT and stolen information from data breaches, could be used to jeopardize intelligence operations. Another case if where Mossad agents were in action. Mossad [in Hebrew: "institute"] has responsibility for human intelligence collection, covert action, and counterterrorism. Its focus is on Arab nations and organizations throughout the world. Mossad also is responsible for the clandestine movement of Jewish refugees out of Syria, Iran, and Ethiopia. Mossad agents are active in the former communist countries, in the West, and at the UN.

The botched operation in Dubai by suspected Mossad agents was one of the notable classified operations exposed and affected by biometri*cs.* In November, 2009, an Italian criminal court convicted 22 CIA agents and one Air Force officer of kidnapping for snatching an Egyptian-born Muslim cleric known as Abu Omar from a Milan street and rendering him to Egypt to be tortured. The 23 Americans were sentenced in absentia to from five to eight years in prison. The discovery of a CIA operation in Milan, where agents left behind many digital footprints, was a prolific example (Hendricks 2010).

Second case study: Open-source information

The case studies that were selected focused on how adversaries can use publicly available information on the internet or other public sources such as court records to harm U.S. cleared personnel and intelligence operations. The study also examined the impact of social media on intelligence operations and the U.S. personnel who work for them. Adversaries use tactics like searching for military and government personnel's names and addresses to target them, similar to those used by ISIS. In recent years, the availability of highly accurate information about government employees and private sector contractors with security clearances has increased exponentially due to the rise of online social networks and user-generated content, which has changed the way people access information on the internet (Ye et al. 2011).

The use of this information inadvertently or by design jeopardized intelligence operations and OPSEC in general, such as the CIA "rendition flights" where detainees were airlifted to locations in foreign countries under the auspices of reinforced interrogations. The exploitation and analysis of social media have also helped opponents of the US in various ways. Facebook is the most popular social networking site; LinkedIn provides more accurate and centralized biographical data on its users who voluntarily provide it. Adversaries have used this data to accurately identify US cleared personnel working on classified programs, make connections and hypotheses with other cleared personnel, and uncover sometimes sensitive operational data about intelligence programs (Ryan 2009.1).

Third case study: The Robin Sage

Robin Sage is a fictional American cyber threat analyst who was created in December 2009 by Thomas Ryan, a security specialist hacker from New York. The name of this fictional character was taken from a US Army Special Forces training exercise. Robin Sage has become a popular figure in the world of cybersecurity. The Robin Sage experiment also demonstrated how social media could be used, in this case, by creating false LinkedIn profiles to recruit and interact with cleared personnel who work on sensitive and sometimes classified government programs. The experiment demonstrated how adversaries might use similar TTPs to create vast networks of online profiles and penetrate the social networks of personnel who work on sensitive programs. Adversaries learn more about these programs that may be available to the public, build targeting profiles, and learn which other personnel work on these programs.

Category III of case studies

First case study: The Intelligence Lifecycle: The third topic will be the Intelligence Lifecycle which is the descriptive model used to account for the main stages of intelligence: orientation, collection, processing, analysis, and dissemination. This Lifecycle is an important element in the proper functioning of intelligence structures and counterterrorism (Kenneth Udokporo, C., 2021).

The Intelligence Lifecycle

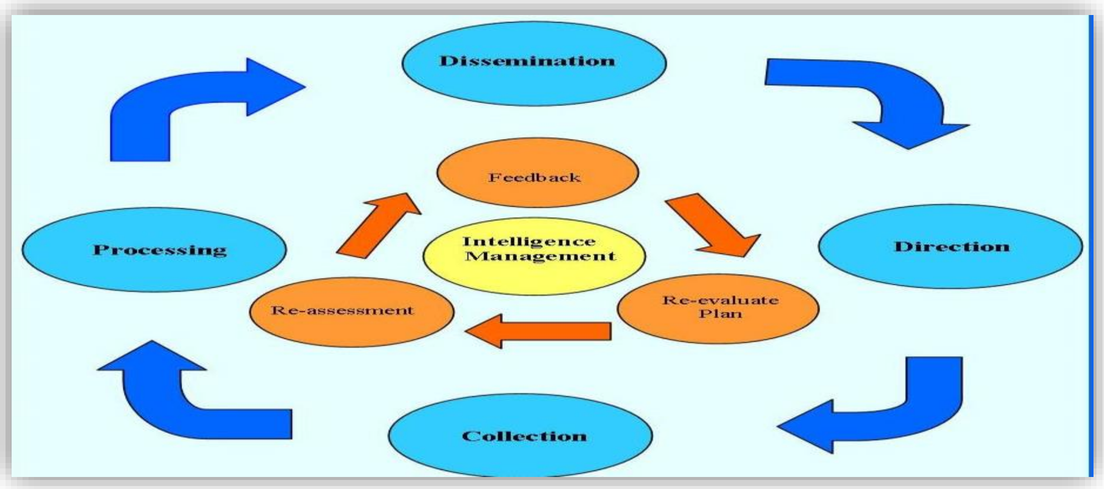


Fig 6: The Intelligence Lifecycle

The Intelligence Lifecycle: How the intelligence cycle works

Step: Collection: Collection refers to the process of gathering information to meet the most important intelligence requirements. There are various ways to gather information, such as: extracting metadata and logs from internal networks and security devices, subscribing to threat data feeds from industry organizations and cybersecurity vendors, conducting conversations and targeted interviews with knowledgeable sources, scanning open-source news and blogs (known as OSINT), scraping and harvesting websites and forums, and infiltrating closed sources such as dark web forums.

The collected data usually comprises finished intelligence information, like intelligence reports from cybersecurity experts and vendors, and raw data, like malware signatures or leaked credentials. After establishing a clear set of requirements, the Intelligence Community proceeds to collect the desired information on the specified subject. Collectors monitor a given target by employing technical or non-technical means, searching for a piece of information that may yield valuable intelligence in the future.

The U.S. Intelligence Community employs various collection methods that work together to create a more accurate profile of a subject. These methods include signal intelligence (SIGINT), which deals with intercepted signals like communications, telemetric information, and electronic emissions. Imagery Intelligence (IMINT) uses visual representations, from outer space imagery to simple photography. Measurement and Signature Intelligence (MASINT) interprets measurable readings like radiation levels and chemical breakdowns. Human Intelligence (HUMINT) collects information from human sources like diplomats or spies. Open Source (OSINT) is a field that gathers unclassified information from sources like newspapers, TV broadcasts, and academic analyses. All these methods are resource-intensive, and managers of different disciplines compete for limited budgetary dollars. Each discipline has its strengths and drawbacks, which are considered in the budgeting process. HUMINT is relatively inexpensive but politically risky and vulnerable to denial and deception. It's often the only way to gather highly specific information, especially about potential adversaries' future intentions. On the other hand, the more technical disciplines like SIGINT, IMINT, and MASINT are relatively more costly but less politically risky than other alternatives.

Collection of intelligence information - targeting and threats

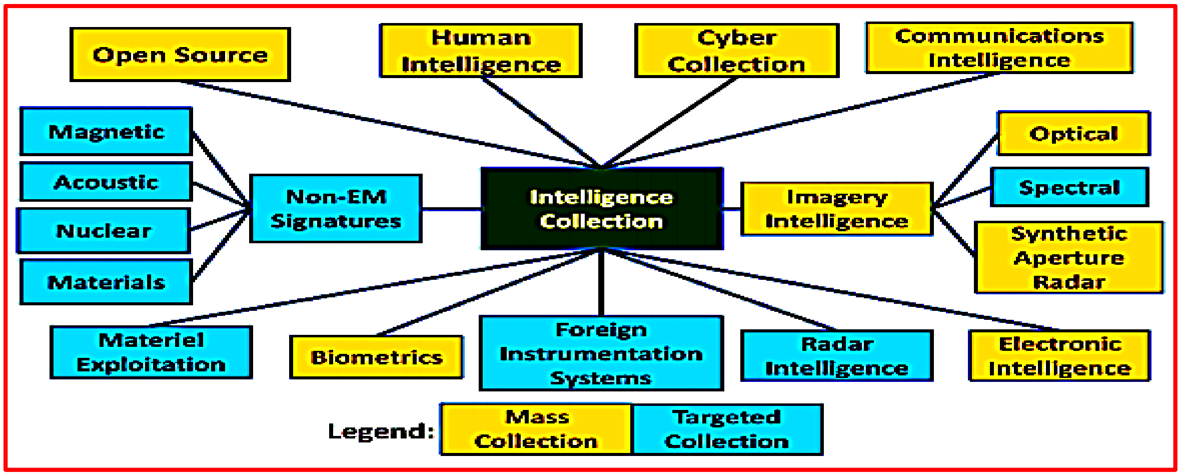


Fig 7: ***Collection of intelligence information - targeting and threats***

Step 2: Processing and Exploitation**:** Processing refers to the conversion of collected data into a format that can be used by an organization. Whether done by humans or machines, almost all raw data collected needs to undergo some sort of processing. Different collection methods often require different processing methods. For instance, human reports may need to be ranked, correlated, deconflicted, and verified. Another example is the extraction of indicators from an email, enriching them with other information, and then communicating with endpoint protection tools for automated blocking.

Collection systems gather vast amounts of data, most of which is not useful. Thus, it is essential to separate relevant information from the rest and present it in accessible ways. This is why processing and exploitation are crucial phases of the intelligence cycle. Their objective is to link collected information to analysts who will examine it. To overcome the challenge of separating signals from noise, skilled specialists must sift through the collected data to find useful intelligence. For example, photo satellites capture thousands of images across the planet, each with varying resolutions, angles, daylight, and weather conditions

Although by its very nature the Intelligence Community always collects more than it processes, there are frequent and perennial concerns that the disparity between the two is unmanageably large. In the halls of Congress, the White House, and the Pentagon, there is a tendency to give greater attention to collection activities than to areas such as processing and exploitation. Much of this involves the relative glamour of high-technology collection projects that promise progressively better technical capacities with each new model.

Step 3: Analysis and Production**:** Analysis is a crucial human process that transforms processed information into intelligence that can help make informed decisions. Depending on the situation, these decisions may include whether to investigate potential emerging threats, what actions to take immediately to block an attack, how to strengthen security controls, or how much investment in additional security resources is justified. How the information is presented is particularly critical. It is pointless to collect and process information and then deliver it in a way that decision-makers cannot understand and use.

For instance, if you need to communicate with non-technical executives, your report must: be concise (a one-page memo or a handful of slides), avoid confusing and overly technical language, express the issues in business terms (such as direct and indirect costs and impact on reputation), and include a recommended course of action. Some intelligence may need to be presented in different formats for various audiences, such as a live video feed or a PowerPoint presentation. Not all intelligence needs to be conveyed through a formal report. Successful cyber threat intelligence teams provide continuous technical reporting to other security teams with external context around IOCs, malware, threat actors, vulnerabilities, and threat trends.

After the information has been collected and screened for relevancy, it is converted into accessible concepts, but it is still considered raw intelligence at best. It is only when this information undergoes the analysis and production stage, where different pieces of information and raw intelligence are combined and evaluated by a team of experts and summarized in a written report, that it becomes finished intelligence. The analytical process is the most important part of the intelligence cycle and lies in the individual analyst's essence.

To ensure the survival of an analytical report, it should abide by four basic principles of good intelligence. First, useful intelligence must be timely as it provides early warning and indication. Even if working with uncertain and fragmented information, analysts should submit an inconclusive report on time rather than wait for more information to arrive. This is to prevent policymakers from learning about developments through the nightly news after an attack or some other significant event has occurred.

Second, a good analysis should convey a clear sense of relative certainty and uncertainty. Rarely does collected information reveal anything approaching absolute knowledge, and analysts should aid policymakers in their strategic calculations by providing them with a degree of confidence in the conclusions of their analyses.

Third, analysts should custom-tailor their reports to the specific policymakers they address. They should craft reports with individual policymakers’ needs and requirements in mind but must avoid losing their objectivity in the process.

Lastly, intelligence reports must be quickly and easily digestible to extremely busy policymakers. This mandates a crisp and coherent writing style.

Competitive analysis is another tool designed to help produce more accurate intelligence. Due to the nature of the intelligence process, doubt and a lack of information at every step can be a breeding ground for errors and misperceptions. As a built-in safeguard, the U.S. Intelligence Community encourages its sixteen affiliated agencies to work on similar issues and discuss their alternate viewpoints. Information is collected, screened for relevancy, and converted into accessible concepts, but it is still raw intelligence. When combined and evaluated by a team of experts and summarized in a written report, it becomes finished intelligence, making analysis the most important part of the intelligence cycle.

To ensure survival, analytical reports should be timely, convey relative certainty and uncertainty, be custom-tailored, and be easily digestible. Competitive analysis is a tool designed to produce more accurate intelligence. The U.S. Intelligence Community encourages its affiliated agencies to work on similar issues and discuss alternate viewpoints.

Despite the best efforts of analytic tradecraft and competitive analysis, there remain many ways in which an analysis can go awry. As part of his or her training, every analyst is warned of common analytical pitfalls that can contribute to flawed intelligence. Such errors include “mirror imaging” (automatically extending one’s own ideas of motivation to other actors), “clientism” (justifying rather than analyzing the actions of the subject of an analysis), and “layering” (building an analysis based on pre-existing, yet faulty assumptions).

Step 4: Dissemination: The process of disseminating finished intelligence involves getting it to the places where it's needed the most. In the field of cybersecurity, there are at least six teams that can benefit from threat intelligence. For each of these teams, it's important to ask questions like what kind of threat intelligence do they need, and how can external information support their work. Also, it's important to consider how the intelligence should be presented to make it easily understandable and actionable for that particular team. Moreover, it's essential to determine how often updates and other information should be provided.

Despite the best efforts in collecting and analyzing intelligence, it doesn't exist until policymakers acknowledge and understand it. The task of distributing finished intelligence to relevant officials is known as the process of dissemination. Most intelligence consumers face a constant barrage of competing information, and policymakers often receive a large number of documents, of which intelligence reports are only a fraction. To meet these demands, intelligence professionals must find ways to customize reports for different types of consumers and present them in a way that conveys the most important information in the least demanding fashion.

Maintaining a systematic and routine flow of intelligence is both challenging and demanding. Senior intelligence officials must first examine which intelligence findings are most important among the many they receive in a given day. They must strike a balance between providing too much and too little information. They must find a way to give policymakers the essential facts they need without overwhelming them with unnecessary details.

Step 5: Consumption: Consumption is a critical stage that is often overlooked in descriptions of the intelligence cycle. It is often taken for granted that policymakers will digest and act upon the intelligence they receive, but this outcome is by no means guaranteed. Some policymakers might discount intelligence that challenges their preconceived notions about a particular issue.

Step 6: Feedback**:** The intelligence cycle has a final and often neglected stage known as feedback, where policymakers assess the Intelligence Community’s performance and provide recommendations for improvement. Two-way communication with policymakers is crucial for activities such as setting requirements and dissemination. It is essential to understand the intelligence priorities and security team requirements for consuming threat intelligence.

These requirements guide all phases of the threat intelligence lifecycle and determine the types of data to collect how to process and enrich it, how to analyze and present it as actionable threat intelligence, and to whom each type of intelligence should be disseminated. Regular feedback is necessary to ensure that the requirements and priorities of each group are understood, and adjustments can be made as necessary.

Threat Intelligence Lifecycle

The threat intelligence lifecycle is the structured process by which threat intelligence is gathered, processed, analyzed, and applied. It's a continuous and iterative cycle that empowers cyber-security teams to predict, detect, and respond to threats with enhanced efficacy. Threat intelligence is built on analytic techniques honed over several decades by government and military agencies. Traditional intelligence focuses on six distinct phases that make up what is called the “intelligence cycle”: direction, collection, processing, analysis, dissemination, and feedback as said above.

The intelligence cycle is a crucial process that transforms raw information into actionable intelligence. Specifically, in the realm of criminal intelligence, this process plays a paramount role in developing finished insights that are useful for policymakers, law enforcement executives, investigators, and patrol officers. These end-users rely on the finished intelligence to make informed decisions and take swift, effective action. In essence, the intelligence cycle is the backbone of a successful crime-fighting strategy, and its importance cannot be overstated.

Threat Intelligence Lifecycle

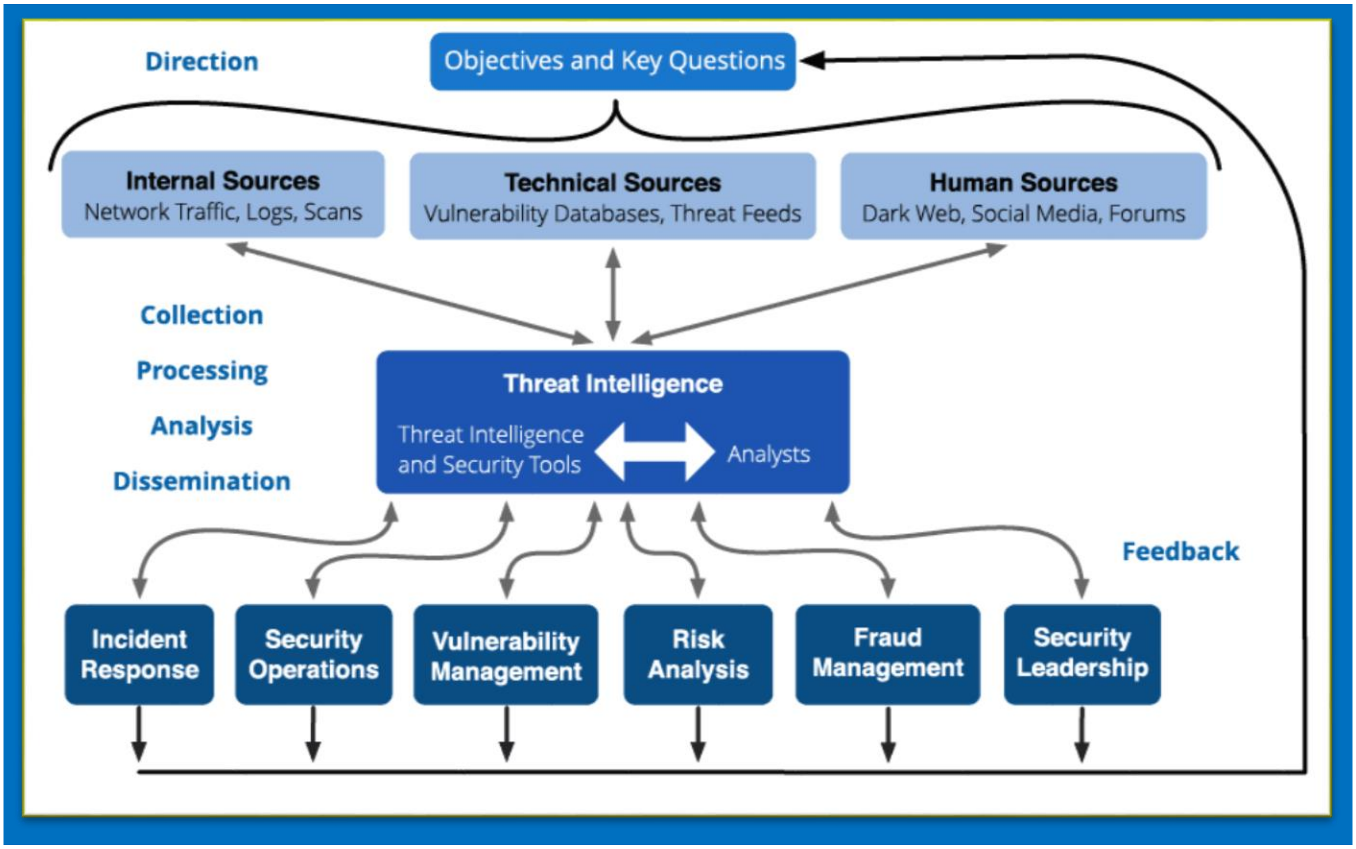


Fig 7: Threat Intelligence Lifecycle

Direction

The direction phase of the lifecycle is when you set goals for the threat intelligence program. This involves understanding and articulating: The information assets and business processes that need to be protected. The types of threat intelligence that the security organization requires to protect assets and respond to emerging threats

Priorities about what to protect

Once high-level intelligence needs are determined, an organization can formulate questions that channel the necessary information toward distinct requirements. The goal is to understand potential adversaries and determine the type of actors who threaten underground forums and actively solicit data about our organization.

What and why the Cyber Threat Intelligence Cycle?

Cyber threat intelligence Cycle crucial for security teams: The cyber threat intelligence cycle is crucial for security teams because it offers a methodical approach to gathering, analyzing, and implementing threat intelligence. This cycle helps in comprehending the threat landscape better, which in turn enables teams to prepare for and respond to security threats more effectively. By following this cycle, actionable intelligence can be generated, which is essential to make informed decisions to improve the organization's security posture against cyber-attacks

***Main benefits of implementing a threat intelligence program*:** Implementing a threat intelligence program empowers organizations with the capability to anticipate, prepare for, and mitigate potential security threats. This program is an integral part of the threat intelligence process, facilitating a deeper understanding of threat actors and their tactics. It thereby enables the threat intelligence team to deliver finished threat intelligence crucial for proactive defense measures. Moreover, a threat intelligence program enriches incident response strategies and fosters a culture of continuous learning and adaptation to the evolving threat landscape.

***Organizations benefiting from the cyber threat intelligence cycle*:** Organizations operating in sectors with high-value data such as finance, healthcare, and government are often prime targets for threat actors, hence they greatly benefit from the cyber threat intelligence cycle. This cycle, with its defined threat intelligence lifecycle stages, aids in intelligence collection and threat intelligence analysis, crucial for understanding and mitigating potential risks. Additionally, organizations with a significant online presence, businesses that focus heavily on uptime, or those subject to regulatory compliance also find the cyber threat intelligence cycle indispensable in navigating the complex security landscape.

Challenges faced when implementing the cyber threat intelligence cycle: The common challenges during implementation include the initial setup of a robust threat intelligence platform, ensuring continuous and relevant intelligence collection, and analyzing data accurately to generate actionable insights. The effectiveness of threat intelligence reports can be hindered by a lack of skilled personnel or inadequate resources. Furthermore, integrating the insights obtained from the threat intelligence analysis into the existing incident response procedures and ensuring a seamless flow of information can also pose significant challenges.

Weakness of Counter-terrorism structures in US-allied countries

US-allied countries, including African countries, do not have a proper counterterrorism system although these countries have immense potential and opportunities. U.S. allied countries and African countries can provide a vital pillar in safeguarding U.S. interests and sovereignty.

Despite their importance, African countries face a multitude of challenges that hinder their contribution to the fight against global terrorism. One of these challenges is technological limitations. Many African countries rely on obsolete equipment, hampering their ability to effectively respond to modern security threats. Many African countries lack access to advanced defense and security technologies, limiting their ability to effectively control their borders, combat terrorism, and respond to emerging security threats. This technological capacity gap not only affects national security but also hinders the continent's ability to contribute to global peacekeeping efforts. Besides technological and financial limitations, the defense industry in Africa also faces corruption and governance issues. Weak governance structures can weaken defense institutions, making them vulnerable to corruption and lack of accountability. Such challenges not only undermine the effectiveness of security forces but also diminish public trust in these institutions.

The diversity of security threats in U.S. allied countries and African countries further complicate the task of an intelligence system designed to combat terrorism. From terrorism and insurgency to transnational organized crime and border conflicts, African countries face a wide range of challenges. Developing comprehensive strategies to address these multifaceted threats requires close cooperation and information sharing among nations as well as direct and sincere support from the United States. Additionally, partnerships with external actors, such as international organizations and advanced defense industries, can provide U.S. and African allies with access to expertise, training programs, and transfer of technologies.

Regional and international cooperation is an important element in the fight against terrorism. By joining forces, U.S. and African allies can create a stronger, more resilient collective defense system against counterterrorism.

Data Collection

Data collection represents information gathered in the form of numbers and text which is done after an experiment or observation. It is a process of collecting and measuring information on variables of interest, in an established systematic manner that allows the research questions posed to be answered, hypotheses to be tested, and results to be evaluated.

All the information for this study came from open-source materials. Cases were discussed came from the event of the kidnapping in Milan by CIA agents, the other information came from the CIA's rendition program. The Inspector General's Final Audit Report served as the most significant government publication on the OPM breach (OPM 2008).

The remainders of case study materials were sourced through, government and private industry reports, and reputable academic websites. Detailed findings and damage assessments on these cases remain classified.

Data Analysis Procedures

This case is being analyzed to demonstrate how enemies, who may be terrorists or countries opposing US policies, can infiltrate the systems of government agencies to steal sensitive information. Reports from the Government Accountability Office indicate that the Office of Personnel Management failed to implement over a third of recommended security measures after suffering from data breaches that lasted for several years. In June 2015, the agency reported that an intrusion by the enemy had compromised the personnel records of around 4.2 million current and former federal employees. This was followed by another breach in July 2015, which affected the agency's systems and files related to background investigations of 21.5 million individuals (OPM 2015).

There are three categories of case studies which are:

Category I Intelligence: (- a) The UK Intelligence, Counter Terrorism and Counter Intelligence services, b) The United States Intelligence, Counterterrorism and counter-espionage services, c) The French Intelligence, Counterterrorism and counter-espionage services; d) The Democratic Republic of Congo's Intelligence, Counterterrorism and counter-espionage services.

Category II: **Internet used** with three specific case studies which are: (a) Data breaches, b) open source intelligence, and c) the Robin Sage affair;

Category III: **Intelligence life cycle**, which are: a) planning and directing - b) intelligence gathering - c) intelligence processing - d) intelligence analysis/production - e) intelligence dissemination - f) information feedback.

To make the diagram easier to understand, not all thirteen case studies will be presented in the matrix. However, the first four case studies will be considered separately from the remaining three. We will expand one column in the matrix to create three questions.

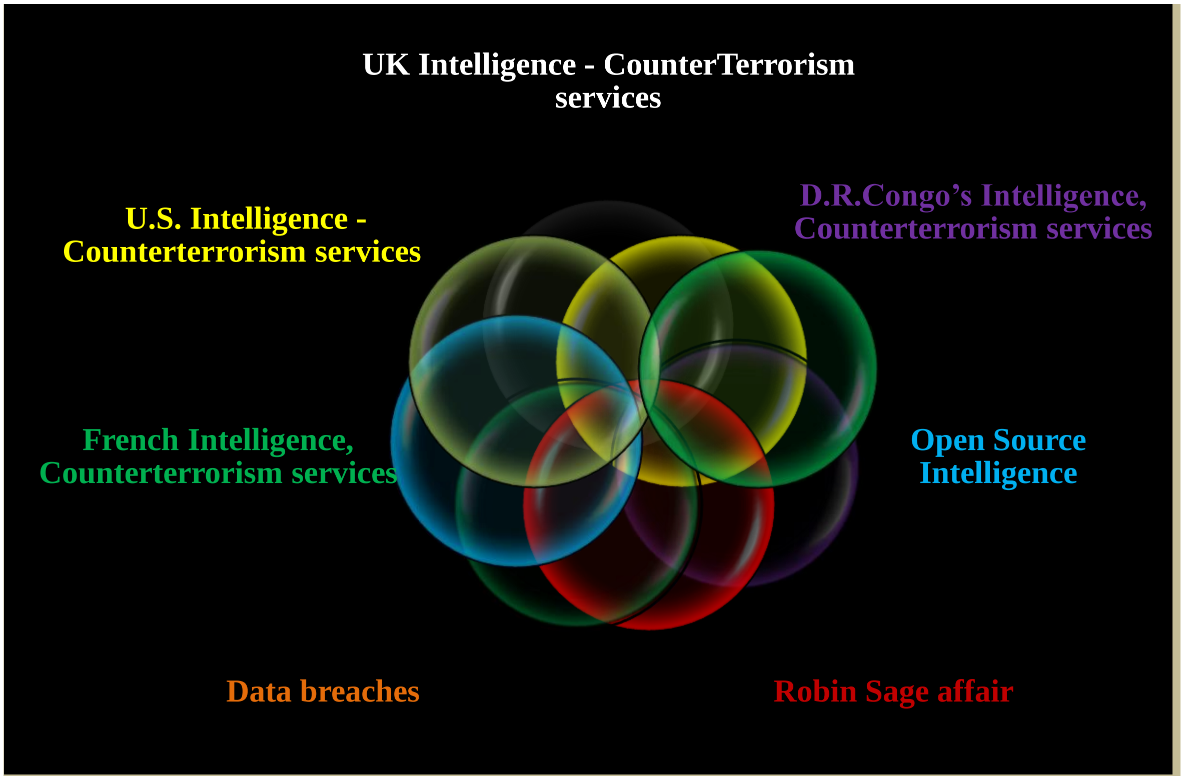
These questions will serve as criteria to determine whether the cases were appropriate for this study. Finally, we will integrate the first four case studies into the matrix.

Seven case studies will be used in this matrix to be analyzed: a) The UK Intelligence, Counter Terrorism and Counter Intelligence services, b) The United States Intelligence, Counterterrorism and counter-espionage services, c) The French Intelligence, Counterterrorism and counter-espionage services; d) The Democratic Republic of Congo's Intelligence, Counterterrorism and counter-espionage services; e) Data breaches, f) open source intelligence, and g) The Robin Sage affair.

These seven cases chosen from the thirteen made it possible to clarify the research question. In today's digital age, the use of biometrics and internet data breaches can have far-reaching consequences. It's not just about personal privacy, but also about national security. The identification of individuals working for counterterrorism missions can put authorized U.S. personnel at risk, while also providing a golden opportunity for terrorists to exploit. Therefore, it's vital that we take the necessary precautions and implement effective security measures to safeguard our country and its citizens. The sketch study above is done to visually aid in the identification of iconic case studies. The integration of biometric monitoring and OSINT into a holistic surveillance strategy is imperative. Failing to adopt this approach may render a surveillance plan incomplete and ineffective. Therefore, it is critical to incorporate these technologies to ensure a robust and reliable surveillance system (Rathee, G., Maheswar, R., Sehar, S. et al., 2023).

The other cases of studies not carried out on the matrix were addressed to show that the countries that search to reinforce their intelligence structure are supposed to have a complete intelligence cycle. The intelligence cycle is a set of processes used to provide information useful for decision-making and includes several processes. Counter-intelligence plays a vital role in safeguarding against third-party intelligence efforts. Without it, sensitive information could fall into the wrong hands, leading to disastrous consequences. Therefore, it is imperative that counter-intelligence measures are taken seriously, and necessary steps are implemented to ensure the protection of sensitive data.

Seven Cases studies



UK Intelligence - CounterTerrorism services

U.S. Intelligence - Counterterrorism services

D.R.Congo’s Intelligence, Counterterrorism services

French Intelligence, Counterterrorism services

Open Source Intelligence

Data breaches

Robin Sage affair

Figure 9: Seven Cases studies

Three categories of case studies (including thirteen specific case studies.

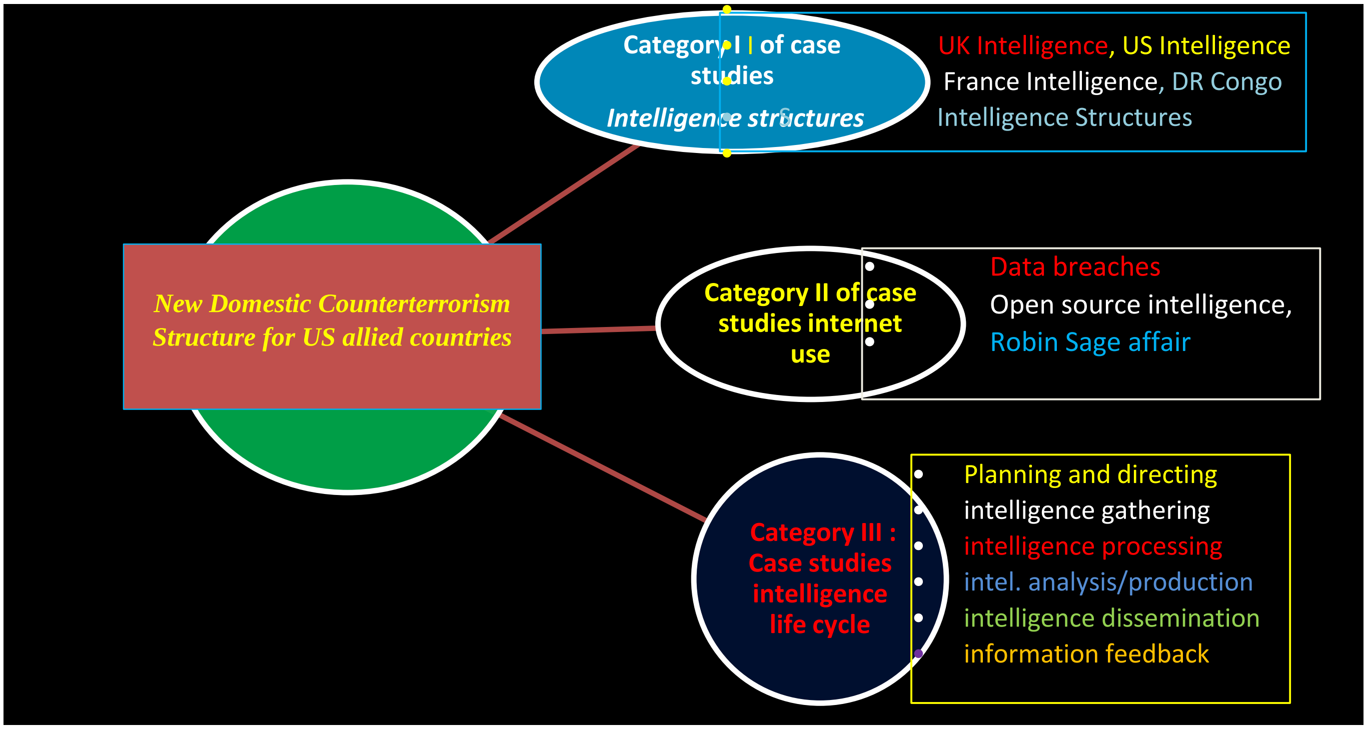

Category I I of case studies
Intelligence structures
UK Intelligence, US Intelligence
France Intelligence, DR Congo
Intelligence Structures
New Domestic Counterterrorism Structure for US allied countries
Category II of case studies internet use
Data breaches
Open source intelligence,
Robin Sage affair
Category III : Case studies intelligence life cycle
Planning and directing
intelligence gathering
intelligence processing
intel. analysis/production
intelligence dissemination
information feedback

Fig 10: Three categories of case studies

Source: Ursoel Mayumbu conception.

<u>Illustration</u>:

Any domestic counterterrorism structure of allied countries should have control over these three categories of threats which are cases of countries chosen to resolve the problem raised in the 13 specific cases which are in particular:

a) British Intelligence, American Intelligence, French Intelligence, DR Congo, Intelligence structures;

b) Data breaches, open source intelligence, Robin Sage affair;

c) Planning and direction, intelligence gathering, intelligence processing, information, analysis/production, dissemination of intelligence, and feedback of information.

Comparison Matrix

Categories of cases	**Intelligence structures**	**Internet use**	**Intelligence Life- Cycle**	**Affected by Data Breach?**
UK Intelligence structure	Strong	Possibly Data Breach	Yes	Yes
US Intelligence structure	Strong	Possibly Data Breach	Yes	Yes
France Intelligence struc	Vulnerable	Vulnerable	Yes	Possibly Data Breach
DRC Intelligence structure	Very Weak	Vulnerable	NO Exist	NO
Sample Countries	UK Intelligence structure	US Intelligence structure	France Intelligence struc	DRC Intelligence structure
Vulnerable to OSINT?	Yes Vulnerable	Yes Vulnerable	Yes Vulnerable	Yes Vulnerable
Robison Affair	NO	Yes	NO	NO
Planning and Directing	Strong	Strong	Strong	Very Weak
Intelligence gathering	Affected by threat	Affected by threat	Affected by threat	Very Weak Only HUMINT
Intelligence Process	Strong	Strong	Affected by threat	Very Weak
Intelligence Analysis	Strong	Strong	Affected by threat	NO Exist
Intelligence Dissemination	Strong	Strong	Strong	Very Weak
Info Feed back	Strong	Strong	Strong	NO Exist

Table 2: Structured Focused Comparison Matrix

The American and British intelligence structures are the leaders and role models in countering terrorism, but France and the Democratic Republic of Congo represent all allied countries. Taken as an example the allied countries' counterterrorism structure and intelligence cycle need to be improved

Assumptions and Limitations of the Research Design

There is a limited number of comprehensive works on the subject of open source intelligence, data breaches, and specifically intelligence operations including biometric detection technologies. Since the details of these data breaches are still emerging and the level of classification of intelligence operations and authorized personnel who may have been affected by this data, the literature is limited to very few articles, government reports and industrialists, on the CIA, rendered flights and details of the kidnapping operation revealed by the CIA in Milan. General reference materials on trade, insider threats, and Cold War case studies that reinforce the thesis were found in four additional books on politics, intelligence analysis, and historical references.

The key hypothesis is that the combined information from OPM and the Ashley Madison website is used by adversaries or terrorists to target counterterrorism personnel who travel (or are stationed) outside the United States. United. The tools available to terrorist adversaries to initially identify these personnel will be biometric technology and screening at airports and points of entry of other adversary countries. Another critical assumption is that aggregated data from previous data breaches will be used to populate biometric databases that will be used to cross-reference travelers at ports of entry.

Finally, the data breach at OPM was likely perpetrated by the Chinese government or by individuals working on behalf of the Chinese government. The information stolen from OPM was not disclosed or sold on the Internet, leading to speculation that the attack was "state-sponsored." The data breaches against Home Depot and Target made their financial data available for sale on the Internet shortly after the intrusions (Finklea 2015).

Since the Chinese and Russians have a cordial relationship, especially on security and intelligence matters, it is presumed that the Chinese will share portions (if not all) of the OPM data on the US cleared personnel with Russian intelligence services. Numerous scholarly publications allude to this fact.

Credibility

The credibility of the cases used in this study was validated by the parent organizations that lost the information. Data from several companies has been stolen or compromised. These companies include the Office of Personnel Management, Insurance, and United Airlines. This information is directly confirmed on the Ashley Madison website. With enough evidence in the public domain that adds credence to the facts of the case, as was highlighted earlier in the literature review.

Transferability

The findings and evidence presented in this study are transferable to the Department of Defense, the intelligence community, and businesses in the United States and those of allied countries, which manage process, and support classified information for the United States government and possible allied countries. By understanding what is not working in each case study, these examples can be “learning points” reported by senior leaders to their parent organizations to improve and avoid future problems. The embarrassing revelation of information and operations from most of these cases can serve as a learning point to prevent future intelligence operations from going as poorly as those in the case studies. Ultimately, the recommendations from this study may already be included in updated TTPs within specific organizations and government agencies.

Ethical Issues

The information described in this study raises ethical issues. However, precautions have been taken not to further harm the true identities of personnel leading the fight against terrorism by the United States whose personal information was stolen or intelligence officers whose identities were revealed due to the recreation of open source recordings by adversaries.

The researcher assumes that the Foreign Intelligence Surveillance Service (FISS) may not be concerned about the harm they cause to US-authorized personnel by accessing Open Source Intelligence (OSINT) and breaching data. The personal information obtained through the OPM breach, as well as website data, could be used to recruit a U.S. spy, even though such an act would be highly unethical. The researcher had the option to mention the names of authorized individuals who are presently working for intelligence agencies, including the CIA, who have been exposed to data breaches or are gathering open-source information from the Internet, just as adversaries have done in the past. By citing specific names, it would be easy to demonstrate how adversaries have used this information to expose authorized personnel and intelligence operations. However, the researcher chose not to reveal the identity or operational details of these cases in writing, so as not to further compromise their security.

Classified information refers to sensitive information that government agencies consider confidential. It includes the security clearances of authorized personnel. In the American information system, there are three levels of classification: Top Secret, Secret, and Confidential, which are defined in EO 12356. Generally speaking, there are four classifications of data: public, internal only, confidential, and restricted. The classification level of restricted information is such that if it is publicly disclosed without the appropriate authorization, it would cause harm to national security.

Summary

The researcher compiled, analyzed, and presented the information with the primary goal of demonstrating that adversaries can use protected data to target personnel working on intelligence missions and fighting terrorism abroad. To do this, the researcher used case studies, selected based on a matrix of criteria identifying them as being vulnerable to OSINT, affected by information from data breaches or compromised due to adversary biometric detection or even showing that in a country allied to the United States there is no counterterrorism structure. Each of the case studies was unique enough to meet at least one of the selected criteria.

The lack of a complete intelligence cycle is a major problem in the fight against terrorism and allied countries that are not better equipped and not supported by the United States live in permanent risk of seeing the terrorist reservoir strengthen and unfortunately, these terrorists are targeting the United States of America. Terrorists' use of open source information gives them the advantage of knowing the people who are fighting them. It is not about individual terrorists but also about countries that support terrorism. This information is appropriate for validating the key points of each case, even if some critical assumptions rely on facts that may still reside within the classified domain and are not accessible to the researcher. Open-source intelligence and biometrics demonstrate emerging tools used by adversaries to expose U.S. personnel. Data from OPM and OSINT violations can contribute to biometric databases that foreign governments use to track U.S.-authorized personnel. Terrorists and the countries that support them know how to identify weak countries where they can form a reserve of fighters and launder money while waiting for the next attack.

CHAPTER FOUR

FINDINGS & ANALYSIS

Introduction

The intelligence structures of several model countries like Britain and the United States are affected by intrusions from enemy countries that support terrorism using open source, which is one of the causes that impact operations. Intelligence personnel who support covert intelligence operations are also affected by the use of open sources by terrorists and other enemies. The same goes for information stolen in data breaches and biometric technology used to identify, target, or expose overt and covert personnel during OCONUS travel.

In this study, the identification of the few case studies that fall into the three categories of studies cited will be examined and concluded. This study will also attempt to understand how adversaries use OSINT, data breach information, and biometric technology to affect intelligence operations and undermine the counterterrorism system of model countries. A discussion of the greatest commonalities between the most significant case study examples in each category and their vulnerabilities will be assessed and concluded.

To strengthen the study cases of data breaches and open source intelligence, in addition to the Robin Sage affair already cited, some emblematic cases are brought together to facilitate the understanding of the audacity of terrorists and the countries which support them in the violation of the 'information from institutions and individuals. Data breaches are becoming a very widespread and daily practice within their reach. Reason why the need to cite these few cases becomes imperative to allow the revision of old intelligence structures that have become obsolete and to put in place new intelligence structures which take into account the internal protection of allied countries against terrorism.

The iconic case studies selected are OPM Breach, Ashley Madison – Website Data Breach, Anthem Health Insurance Data Breach, United Airlines Data Breach, CIA Reveals Milan Operation, Revelation of the CIA on the rendition plane operations and the Israeli Mossad denounces a kidnapping operation.

ICONIC CASE 1: OPM Breach

Research was carried out and a damaging discovery was made in relation to information obtained from the Office of Personnel Management data breach in 2015. This information was the most damaging to the Intelligence Community to date. The information stolen will initially impact the US cleared personnel and ultimately impact intelligence operations once the information is aggregated to biometrics systems and further analyzed by adversaries. What catches the eye is that the U.S. government's Standard Form 86 on individuals were stolen and these documents contained the biographical details and other PII for everyone who applied for a security clearance. The details within the forms included the applicant's PII, information on their families, foreign contacts, associates, travel history, educational history, criminal activity, drug use, and other sensitive information related to their private lives.

The US security clearance is approved after submitting the US Government Form 86 for review. The SF-86 states that "the government of the United States conducts background and additional investigations of persons considered or detained in national security positions as defined in 5 CFR 732 and for positions that require in-depth access to information under Executive Decree 12968." This SF-86 form is voluntary and guarantees the candidate's eligibility (OPM 2016).

By lying about the information on the form, disqualification is automatic and becomes a punishable offense. As a result of the investigative process, a formal interview is sometimes conducted to allow the applicant to provide updated or more specific responses to questions about the SF-86.

Investigations are made to detect if the personnel concerned is involved in any activation which could prove harmful to the security of the national territory. The initial investigation of a new applicant can last from six months to a year. A security clearance is valid for five years. Three months before the five-year expiration date, a review process is initiated. The review process can be completed by an OPM investigator within 6 months. If the investigation is open, the requester (if it is a new investigation) can continue to access it even if the five years have expired (OPM 2008).

Opponents will most likely use the stolen OPM information to target the US cleared personnel who conduct and support intelligence operations. When adversaries have sufficient biographical and general data on cleared personnel, they will be able to trace the life of that person. When that person's life is mapped out, the adversary will have a full understanding of personal traits, habits, weaknesses, strengths, and other attributes. This information is essential for adversaries to develop a targeting plan to blackmail, recruit or otherwise neutralize the capabilities of that cleared person who belongs to a specific operation or intelligence program.

Due to the failure to protect sensitive and sensitive information, theft occurs, as an example of information stolen during the OPM breach also including foreign contacts and foreign travel. If Chinese intelligence services automatically use information from the SF-86, they will know exactly which intelligence officer spoke to this or that individual, or whether and when that officer visited China.

The Chinese could then track down these Chinese nationals (some of whom could be American IC agents spying on their own country) and neutralize their usefulness to the Americans. Chinese national intelligence could target this family of assets for retaliation and transmit false information about this asset to provide to the Americans, along with a host of other offensive counterintelligence operations that are believed to have useful implications for the effectiveness of US intelligence missions involving China. Dmitri Alperovich is the founder of Crowd Strike; he believed that Chinese hackers were using information obtained through breaches of the US Office of Personnel Management, as well as intrusions into Anthem's health insurance networks. This would create a comprehensive profile of federal employees in what the company calls a “Facebook of Everything” (Herridge & Dean 2015).

The Chinese would therefore have the upper hand in identifying US-authorized personnel or in reconstructing intelligence operations with the help of OSINT. Biometric identification technology has advantages and should therefore be used at border checkpoints to identify authorized U.S. personnel based on information contained in what they call the "Facebook of Everything." China's "Facebook of Everything" stems from their view of intelligence collection as "a thousand grains of sand", where Chinese intelligence officers would recruit agents with limited functions in a host country to collect only a little information (Hannas, Mulvenon, and Puglisi 2014).).

Information that does not go back to the source does not allow for easier and faster data analysis. However, when the information is compiled together, it forms a complete picture or “range” (Hannas, Mulvenon, and Puglisi 2014).

The SF-86 information details all the places whose cleared personnel went to school and who their employer was during the past seven years. Such information is valuable to adversaries, especially if it is used in conjunction with biometrics at border crossing points. If the information stolen from the OPM violation is aggregated and used as a reference database in biometrics software, such as fingerprint readers, iris scans, or facial recognition, adversaries are at stake instantly if the US-cleared personnel arrives in their country under an alias identity or their real identity.

In any case, the intelligence services of the host country could immediately begin surveillance or other control operations against the US-cleared personnel while in the country. If the cleared personnel is there for an intelligence operation, as in the case of recruiting or meeting a local asset, this mission is now compromised. The ramifications of this asset would also be quite dire, especially in China where espionage laws are more severe than in the United States. If the US-cleared personnel is in that country on vacation, for example, the host country's intelligence service could also target the officer for recruiting, blackmail, or other adverse action, especially if it finds out that the individual has an addiction to gambling, drugs, alcohol or sexuality that was on their SF-86.

The vulnerabilities exposed in OPM's data breach case study are poor network or computer software security in U.S. government databases and centralized storage of the most critical data on authorized personnel by the United States in databases connected to the open Internet. Additionally, OPM may choose in the future to segregate SF-86 data so that it is not centrally stored in one place for adversaries to attack.

Many leading experts believe that China-affiliated hackers should be the culprits for the OPM violation. The damage has caused irreversible harm to US-cleared personnel and, ultimately, to the intelligence operations they support. Generations of intelligence officers, analysts, and other support staff have been permanently compromised and the ramifications of this monumental data breach will continue to be felt for very long periods.

ICONIC CASE 2: Ashley Madison - Website Data Breach

The private data of more than 33 million users worldwide was stolen from Ashley Madison's computer networks (July 2015) by a hacking team called "The Impact Team" (Farmer 2015).

The stolen information combined with data from the OPM breach as well as from Anthem and United Airlines (discussed in the following sections) presents a very complete picture of who in the authorized community may be vulnerable to snooping or change if they were members of this website. The Pentagon is also researching the list of leaked clients and their sexual preferences on Ashley Madison's cheating website to identify members of the service who may have broken military rules against infidelity and be vulnerable to extortion by individuals of foreign intelligence agencies (Bennett & Hennigan 2015).

Ashley's data could be plugged into China's “Facebook of Everything” and become an even more comprehensive database used to target the US cleared personnel. The House Intelligence Committee's top Democrat, Adam B. Schiff, also said the huge data treasures could reveal problems that foreign intelligence services could use to identify and target someone for blackmail activity or espionage (Bennett and Hennigan 2015).

Due to the emerging situation in November 2015, there is little analysis of unclassified official government reports. Members of the DoD and IC were reprimanded, fired, or forced to resign because of the incident, which affected all supported intelligence operations.

ICONIC CASE 3: Anthem Health Insurance Data Breach

Private information has been stolen from medical records, such as in the case of the health insurance company Anthem. This information also helps adversaries identify vulnerabilities in the US-cleared personnel (Constantin 2015).

Once these vulnerabilities are identified, FISS can use this information to blackmail or recruit the US-cleared personnel and turn it against the United States for espionage purposes if the health issues exposed are embarrassing to the public or his family. In February 2015, Anthem was the victim of a cyber-breach that affected approximately 78 million people. The company failed to encrypt the data and succumbed to simple phishing attempts, where fake emails were sent to IT pros who clicked on links allowing backdoor access to adversaries of their systems (Hiltzik 2015).

Phishing attempts are a common TTP used by criminals and other hacking organizations to persuade individuals to click on their malicious website link in an email. Typically, only a small percentage of users who receive phishing emails open them, but it only takes one user to let the adversary gain access to the network. Hackers assume so, which is why they send so many emails. The medical information stolen from Anthem has yet to appear on the black market, indicating that the attack was mostly state-sponsored and not carried out by for-profit criminals who, in turn, would sell the information on the black market (Bennett & Hennigan, 2015).

This TTP is like the OPM violation because this information also did not appear on the open market for sale. These two data breaches led many IC members to suspect the Chinese were responsible for the two attacks, possibly as part of a coordinated attack, as part of a larger plan to target the new US cleared personnel and their most sensitive information.

ICONIC CASE 4: United Airlines Data Breach

According to the Director of National Intelligence, James Clapper, the Chinese were able to penetrate the computer networks of the company United Airlines. Given that United is a major supplier of US government travel, this Chinese attack would mean that a vast cache of information about the movements of some government or military officials is now in the hands of the attackers (Peterson 2015).

Referring to comments from former senior FBI cybersecurity and technology adviser Paul Tiao, the stolen information could be used in conjunction with OPM and Anthem data to potentially blackmail or coerce the cleared personnel into committing a crime (Peterson 2015).

When an intruder bypasses the security mechanism, their action violates the security protocol, resulting in unauthorized access to computer data, applications, networks, or devices. In this case, the severity of the breach affects all intelligence operations. The information would be valuable to adversaries as it could collect past trips of the US-cleared personnel. This travel history could be crossed with the entry and exit records of the conflicting country to determine if the person who flew in their country was using a pseudonym or their real name using biometric detection as well as other OSINTs. The ramifications to past intelligence operations whose support personnel have been jeopardized by this breach could be serious for future operations.

ICONIC CASE 5: CIA Exposure of Milan Operation

Data breaches of sensitive information on the US cleared personnel are of great concern, therefore, complacent CIA agents have left an important digital trail in the hands of enemies.

Hassan Mustafa Osama Nasr, known as Abu Omar, is a radical imam living in Egypt, an alleged militant of Al-Gama'a al-Islamiyya. He is one of the leaders of a very committed group with a specific goal of overthrowing the Egyptian regime and replacing it with an Islamic state. He was kidnapped in early 2003 by CIA officers in Milan, Italy (Hendricks 2010).

Hassan, who was a suspected terrorist, was freed in the first years after the September 11, 2001 attacks, but what made this case so important was the ease with which 22 CIA agents were discovered by the Italian authorities.In this case, it is understandable that the Italian government had to use several biometric fingerprints left by the CIA team to uncover Abu Omar's kidnapping in Italy. The most egregious results were the repeated use of the same subscriber identity module, known as SIM cards and phones used by the CIA near the kidnapping site (Fisher 2013).

The US-cleared personnel supporting intelligence in Italy have purchased a SIM card forgetting that it is customary when purchasing a SIM card, it has requirements such as presentation of identity cards before the purchase. The Italian authorities traced the SIM cards to the stores that sold them, and copies of several passports were discovered (Hendricks 2011).

Although some of the passports were fake, but the photos on the IDs were officers. Additionally, by digitally tracking where SIM cards were used in the city through cell phone tower recordings, Italian investigators were even able to locate hotels where agents were staying, and some phones even received calls from CIA headquarters in Virginia (Fisher 2011).

When US-cleared personnel go on missions using false identifications, these individuals cannot use their personal credit cards or other benefits associated with their own identity. From there, hotel files were discovered with the identities of the agents and front companies they claimed to work for. Some CIA agents even used their hotel loyalty point numbers in their real names, exposing and endangering their identity (Hendricks 2011).

Based on hotel registration data, investigators (and later Steve Hendricks, author of Kidnapping in Milan) were able to track down the CIA front companies the agents claimed to be working for as false cover. Italian authorities were even able to determine which flight Abu Omar was taken out of the country from by examining the relative positions of SIM card users concerning the proximity of the US military base and CIA officers (Hendricks 2011).

The identification problems could have been avoided if the CIA agents had not abused their security methods. Good OPSEC practice involves a five-step process: Identify critical information, analyze the threat, analyze the vulnerabilities of the operation, assess the risks, and apply the appropriate security measures (US Department of the Army 2014).

If CIA agents had instead used cash rather than credit cards to pay for hotel rooms, CIA agents might have had the advantage of covering their tracks against Italian authorities by finding out where they were. By changing SIM cards and using other mobile phones, the Italian authorities have also reportedly found it more difficult to follow in their footsteps. Sacrificing a few hundred hotel loyalty points would have prevented the discovery of their identity and their past travels. CIA agents who participated in the kidnapping of Abu Omar experienced dark episodes. Several of these officers were arrested one after another on their trip to Europe. These arrests show the failure of operations carried out by CIA agents and demonstrate the effectiveness of the biometric system set up by the Italian services, which the US had neglected.

As a general rule, except in special circumstances, any legal action involving US citizens should be conducted in absentia. In the Abu Omar case, the United States should not extradite the CIA agents and the Italian government had not issued the extradition request either. The 22 CIA agents were tried in 2005 in absentia for the kidnapping of Abu Omar (Donadio 2009).

Almost eight years later, in 2013, Robert Lady, the head of the CIA station in Milan who was leading the operation, was arrested in Panama at a border crossing with the use of technology biometric identification, on the arrest warrant (Fisher 2013).

Almost 10 years later, in 2015, Sabrina de Sousa, another CIA agent convicted in absentia for participating in the Milan kidnapping, was arrested in Portugal at a border crossing using technology biometric identification, on the Italian arrest warrant (Kowsmann 2015).

Since the operation took place in 2003, at least two CIA agents have been initially identified using biometric technology and temporarily apprehended. Presumably, if the rest of the CIA agents choose to travel outside of the United States and go through a biometric screening process, they can also be identified or even extradited to face Italian courts.

ICONIC CASE 6: CIA Exposure of Rendition Aircraft Operations

Open source is also responsible for information leaks, in which case the Federal Aviation Administration's flight data is provided to several online websites which, in turn, produce real-time information on the locations of planes around the world. These publicly available online databases also provide advance notice of aircraft landings at airports. In addition to online flight databases, flight plans posted on the internet could all be searched to reconstruct past flights from the United States (Gray 2006).

The security of these sites was ignored when it could have allowed for the anonymity available on these flight tracking sites used by the CIA or its contractors who coordinated these return flights. “Time and time again, they seemed to ignore the most obvious ways to secure their operations” (Gray 2006).

Even the identities of the company executives listed in several of the CIA's front companies were all the same, thus linking seemingly different aerospace companies and contractors in different states. Once the names of the front companies and agents were discovered, open-source research uncovered specific flight logs that revealed even more details about the CIA flights and the companies that organized them (Gray 2006).

Using OSINT to track future CIA flights, for renditions or other sensitive intelligence missions, would not allow hostile nations or even terrorist groups to prepare at the landing site to compromise the operation by example. Airplanes, the companies that support them, and U.S.-authorized personnel could also be targeted based on available open-source documents. The denunciation of CIA flights has so far been used by journalists or former detainees to embarrass or sue the US government. Some academic research has been done extensively to demonstrate the risks of open sources. A collaborative research initiative (TRP) led by two professors from the Universities of Kent and Westminster in England has successfully used several open-source methods to track and analyze CIA rendition planes and the front companies that operated these flights. Their website even states that this site's in-depth analysis is supported by an unrivaled body of primary documents, such as prisoner testimonies, declassified documents, flight records, company invoices, and court documents. These elements help to build an unprecedented picture of the CIA's torture program.

Using open-source information, TRP accurately compiled a database of over 11,000 rendition flights, identified over 60 prisoners’ transfers corresponding to flights, and discovered several companies operating these flights on behalf of the CIA (The Rendering Draft 2015).

Despite its best efforts, the CIA did not intend to reconstruct its shell companies and the flight paths of its planes so easily based on open-source information available to the public. In 2003, a billing dispute between two aviation contractors prompted the TRP to start compiling open-source information about the CIA Sportsflight, a New York-based small aircraft brokerage that sued Richmor Aviation in 2003 for breach of contract (Finn & Tate 2011).

These two virtually unknown companies inevitably revealed the first clues to these classified thefts that appeared in court records. Their employer, the CIA, used Sportsflight and Richmor to coordinate and conduct rendition flights for several high-value detainees in the early years following the September 11, 2001 attacks. While details of some of the flights were protected by state secrecy, more than 1,500 documents from the court of first instance and appeal revealed several embarrassing facts (Finn & Tate 2011).

Two relatively unknown companies must have revealed the first indications of these classified thefts which were contained in the judicial archives. The CIA must have used these Sportsflight and Richmor companies to coordinate and conduct rendition flights for several high-value detainees in the early years following the September 11, 2001 attacks. While details of some of the actual thefts were protected by state secrecy, more than 1,500 documents from the court of first instance and appeal revealed several embarrassing facts (Finn & Tate 2011).

These newspapers show several calls to CIA headquarters; the cell phones and personal phones of a senior CIA official involved in the rendition program; and a government contractor, DynCorp, based in Falls Church, who worked for the CIA (Finn & Tate, 2011).

Court documents from that trial were one of many sources of information used by TRP to recreate the flight paths of CIA rendition flights. While some may argue that the TRP is not an adversary of the United States, they have nonetheless succeeded in exposing and reconstructing the CIA rendition flights that forced President Obama to reassess and heavily regulate the frequency of these operations formerly classified as very sensitive.

ICONIC CASE 7: Israeli Mossad Exposure of Kidnapping Operation

There was the emblematic case of Mahmoud al-Mabhouh, who was the top Hamas commander, who was killed in his hotel room in Dubai in 2010. The significance of this operation was that the alleged Hamas team Israeli Mossad who had carried out the assassination was quickly identified using biometric technology and other digital forensic evidence left throughout the city. Just as in the circumstances that exposed the CIA operation in Milan, the Israelis were smart enough to never use their real names on travel documents, credit cards, or any other identifying information. Local authorities were able to determine that fake passports had been used by agents to enter the country. Their real photographs have been broadcast around the world. More than 27 intelligence agents were exposed using biometrics to build a timeline with cell tower records, airport immigration records, credit cards, and surveillance footage (Brannen 2015).

Many groups have conducted investigations, including the Chicago Tribune, which analyzed recordings of the operation in depth. Using database search tools, they discovered more than 2,600 CIA employees, 50 internal agency telephone numbers, and the locations of around 20 secret CIA offices in the United States (Lord 2015. 686).

The agents involved in the revealed operation are unlikely to be able to carry out similar operations in Dubai, as their actual biometric data is now permanently recorded.

Data and Analysis

The comparison matrix that was created aimed to visualize the most important case studies that must have affected intelligence operations and determine whether the information was valuable to adversaries. These results linked to the comparison matrix were weighted based on a maximum total score of 6 per column. A "YES" in the column was weighed as "1" and a "NO" was weighed as "0".

The total results have been reported at the end of each row and column. The first column of the matrix entitled “Information available online” received a score of 5 out of 7. Each of the rows in the column received a score of “YES”, except for the first and the fourth which gave the note "NO". The OPM Breach line was marked as such because as of November 2015, information stolen from OPM was not being published anywhere on the internet. The remaining lines were marked "YES" because each contained data available online to adversaries directly affecting intelligence operations. The second column titled “Information from data breaches” received a score of 4 out of 7 possible. The OPM, Ashley Madison, Anthem Insurance, and United Airlines case studies all scored a "1" (or yes), while the CIA and single-line Mossad case studies scored a "0" (or no). The United Airlines row only had one “NO” in the “Information available online” column because the data had not yet appeared online. The last three operations had information online for opponents, but their operations were not compromised due to a specific data breach.

Structured Focused Case Study Matrix

		Summary	of	Adverse	Impacts		
		Information Available Online	Information from Data Breaches	Affects Intelligence Operations	Affects Cleared Personnel	Enhances Biometric Detection	Overall Score
	OPM Breach	NO	YES	YES	YES	YES	4/5
	Ashley Madison Breach	YES	YES	NO	YES	YES	4/5
ICONIC CASES	Anthem Insurance Breach	YES	YES	NO	YES	YES	4/5
	United Airlines Breach	NO	YES	YES	YES	YES	4/5
STUDIES	CIA Exposure (Italy)	YES	NO	YES	YES	YES	4/5
	CIA Exposure (Aircraft)	YES	NO	YES	YES	YES	4/5
	Mossad Exposure (UAE)	YES	NO	YES	YES	YES	4/5
	Overall Score	5/7	4/7	5/7	7/7	7/7	

Table 3: Matrix of Case Study

The third column also follows the same course of ideas that got 4 out of 7. The OPM breach has been covered extensively in previous chapters and the main reason it got a "1" is because of the loss PII for everyone with a security clearance. Ashley Madison's adultery website breach and Anthem insurance data breaches were significant, but they did not specifically jeopardize intelligence operations. The information, when aggregated with OPM data, collectively advocates affecting authorized personnel but not directly its intelligence operations. The two CIA case studies and the Mossad line were all marked with a "YES" because each mission had specific variables that adversaries used to impact their operations.

The fourth column of the comparison matrix scored a maximum of 7 out of 7 for the impact on intelligence operations by adversaries. Each case study presented a series of issues that affected the US-cleared personnel, such as sloppy operational security, complacency, poor trades, poor IT security, or a host of similar variables.

The fifth column also ranked a maximum of 7 out of 7. The information from each case study could all be used collectively by opponents to enter data into their biometric databases. When information is stored, aggregated, analyzed, and quickly referenced, it creates a monumental counterintelligence threat to the US cleared personnel and intelligence operations.

The sixth and final column ("Overall Score") gave interesting results, with each row ranked 4 out of 5. Each row had at least one "NO" starting with the OPM violation and the United Airlines violation, as the data for both case studies have yet to appear online. Insurance data breaches Ashley Madison and Anthem both had "NO" under "Affects intelligence operations," while CIA operations and the Mossad mission had "NO" under "Information from data breaches ". None of the case studies ranked all "NO" in the rows, and no case studies ranked all "YES" in the row. This is a valuable point, because the data demonstrates that while no one case study is crucial, all the data combined creates a significant problem for cleared personnel, which ultimately affects intelligence operations. The most significant case study within the matrix is the OPM data breach failure. The main reason for this is because the biographical data and other PII for everyone who holds (or held) a security clearance is already aggregated into one organized file called the SF-86 as mentioned earlier in this chapter. The information contained within each SF-86 is of greater value to foreign intelligence agencies and other adversaries than the information from the rest of the case studies combined.

Observation From Case Studies.

From the analysis of the data and the Comparison Matrix on the most emblematic case studies that must have impacted intelligence operations, three observations emerge:

First, gathering information can be costly and time-consuming, and can pose risks, such as the risk of exposure, retaliation, or unintended consequences. The collection of information must ensure the accuracy and reliability of the information collected. At the collection level, several agencies use HUMINT as a collection model and need to involve collection using artificial intelligence.

Secondly, it has been observed that some countries with intelligence structures rely solely on HUMINT or very little on artificial intelligence (IA), or they rely solely on OSINT. This results in imprecise analysis of information since the intelligence cycle cannot function effectively under these circumstances.

Countries such as the UK and the USA should not only protect their borders but also strengthen the intelligence systems of allied countries to prevent terrorists from migrating to low-security countries. These terrorists can continue their illicit activities such as money laundering, kidnapping, organ trafficking, and even training domestic terrorists in host countries.

Thirdly, foreign countries do not have a good collection system in place. The intelligence cycle should have a reliable and cost-effective collection system that can provide accurate information in a short time frame. The speed of collection and analysis enables decision-makers to make informed decisions regarding the security of their countries.

Counterterrorism Intelligence Structure for U.S. Allied Countries Abroad

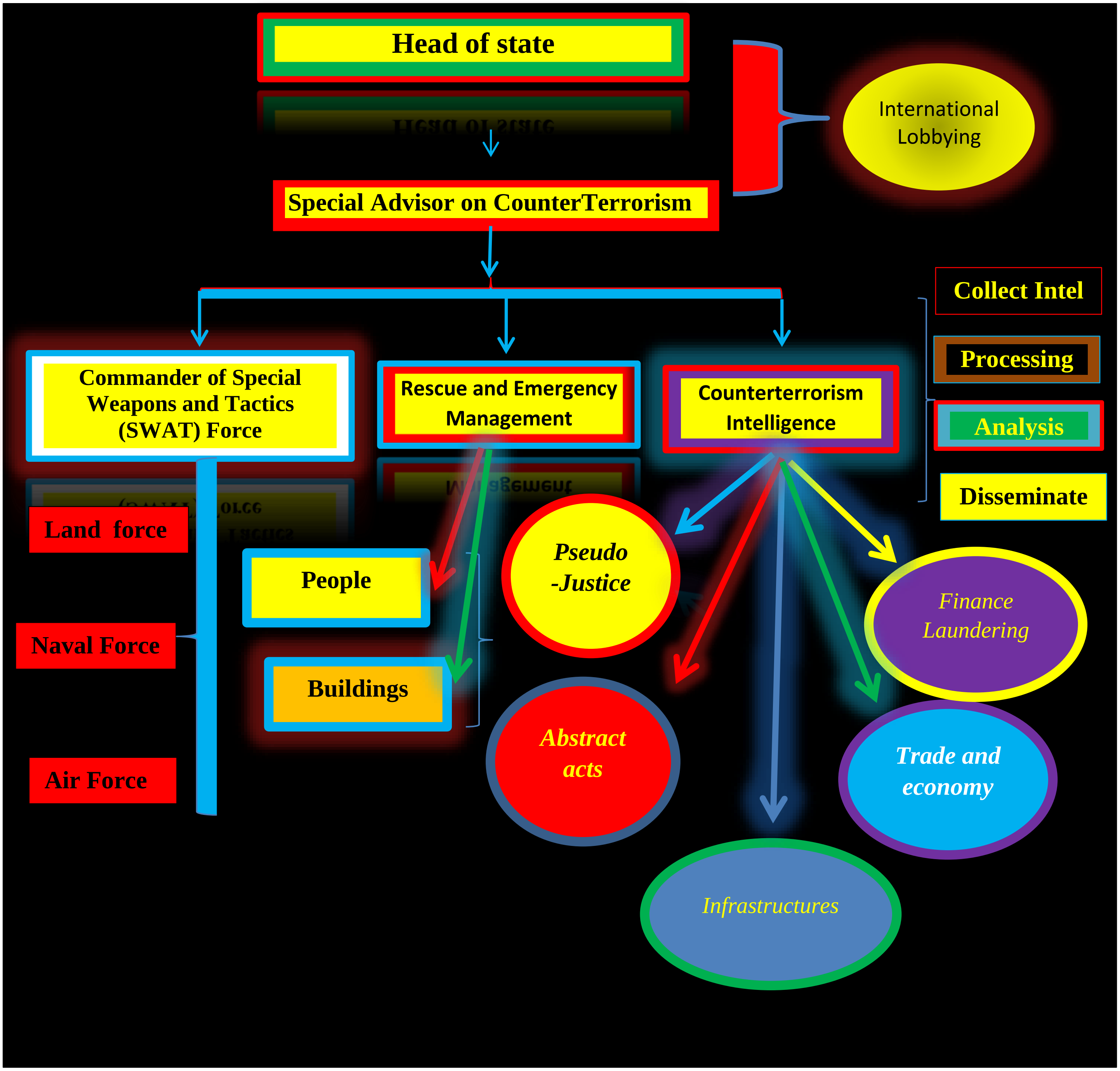


Fig 11: Counterterrorism Intelligence Structure for U.S. Allied Countries Abroad

Source: Ursoel Mayumbu conception

Counterterrorism Intelligence structure for U.S. allied countries.

The scenario of this structure was designed to benefit the countries allied with the United States. The structure refers to the framework established by a group of countries to combat terrorism. It involves cooperation and coordination among the participating countries to identify and prevent terrorist activities. This structure helps the study understand why so many allied countries, which are mostly underdeveloped African countries, Middle Eastern nations, and some European countries, need a specialized domestic structure to combat terrorism.

The heads of state of these countries have broad decision-making powers to respond to any emergencies related to terrorism. To combat this restrictive matter, a dedicated service is placed directly under the responsibility of the head of state of the country, assisted by a special advisor who plays the role of diplomat and popularizer to rally other friendly countries to support the cause of the allied country affected by terrorism.

An activity control structure will be put in place and headed by an intelligence inspector who can collect, analyze, and disseminate information to the decision-makers. In case of an attack, the armed structure will be available and trained in the fight against terrorists and the protection of individuals and infrastructure.

To contribute to the development of a global plan to combat terrorism, a lobbying system at the level of the presidency can be initiated. This system can help obtain grants and access to technical expertise from better-equipped countries. It can also participate in calls for support for other friendly countries in the fight against terrorism..

Summary

The findings presented in this chapter emphasize the significance of every case study and the potential of the collected information for analysis. The chapter proposes a suitable framework to counter terrorism, which can intercept and eliminate the information collected that can be used by adversaries to attack allied countries and the United States before the enemy can leverage it for their benefit.

Based on the case studies reviewed, the use of open-source intelligence, data breaches, technology vulnerabilities, or a combination of these factors had an impact on intelligence operations and authorized personnel supporting covert operations. However, the impact was not devastating and in fact, remained positive

Each case study had a significant impact on the intelligence operation undertaken during the mission. The consequences of these case studies will have a lasting effect not only on the current operation but also on all future operations. It will help avoid repeating the same mistakes in the future. A matrix has been produced, which summarizes the adverse reactions and highlights the factors that influenced each of the case studies.

The case studies suggest that it is crucial to establish a national structure in each allied country, with the support of the United States, to aid these countries in participating more effectively in the fight against global terrorism. It is also important to ensure the protection of the United States, which is considered a primary target by terrorists who seek to violently eliminate all foreign and secular influences in Muslim countries, which they deem as corrupt.

As nations face a range of complex threats to their people and interests, it's essential to work together to protect the homeland from foreign-based and foreign-inspired terrorism, foreign intelligence activities, homegrown violent extremism, transnational organized crime, cyberattacks by foreign agents, and much more. While cyber espionage is a growing threat, traditional espionage remains a means of stealing secrets. The ability to focus technology on less protected information poses a significant risk.

In the United States, the domestic approach to national intelligence involves key roles and relationships that characterize the efforts of members of the American Intelligence Community (IC) and federal, state, local, tribal, and government organizations. These partners work together through established channels with the private sector, such as owners and operators of critical infrastructure, as part of a complex network of relationships. Allied countries should follow the framework and recommendations that are set out in the National Criminal Intelligence Sharing Plan.

Transnational organized crime poses a significant and growing threat to national and international security, with disastrous consequences for public safety, public health, the security of democratic institutions, and economic stability throughout the world. Detecting and attributing these threats can be difficult, as many of them have low-level signatures.

One of the reasons why the United States should strengthen the protection of allied countries is that several countries and numerous foreign intelligence entities consider the United States a priority intelligence target. While traditionally the threat weighs on political, military, and diplomatic interests inside the United States and abroad. The loss of sensitive economic and technological information poses a growing threat to national security.

CHAPTER FIVE

CONCLUSIONS

Introduction

It is not in the interest of the United States for its allied countries to have weak security and defense systems. The stronger the parent country, the better equipped its allies are to maintain a balance of power in regions where the United States cannot secure its interests. To achieve this, intelligence agencies of allied countries should develop a multifaceted system of collection that is comparable to the systems of leading countries such as the UK and the USA.

The intelligence cycle is a process that involves obtaining, producing, and providing intelligence to users. In the United States, this cycle is described using a five-step process, while other nations may have their own descriptions. Adversaries use several intelligence disciplines to gather information about countries, including Human Intelligence (HUMINT), Electromagnetic Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), and Open Source Intelligence (OSINT).

Various disciplines are utilized by developed countries like the United States to gather intelligence on their adversaries and competitors. Many subnational and private organizations, as well as most countries, have their own capabilities to gather data. Because of the openness of American society, open-source intelligence proves successful in targeting the United States. Technical and professional journals often provide valuable information about a country's government and business activities. The search parameters used for these databases can be structured to extract only relevant information for analysis. As more and more information becomes available electronically, the collection of open-source intelligence (OSINT) poses an increasing threat.

OSINT is used by intelligence agencies to track events, equipment (such as weapons systems), and people. It is often referred to as the “Targets of Interest” (ToIs) method of collecting. Hackers also use OSINT to identify technical vulnerabilities and human targets for phishing and social engineering attacks.

Open-source intelligence is one of the cheapest and most easily usable tools that adversaries can use against US-cleared personnel who conduct and support intelligence operations. By targeting these individuals, adversaries can negatively impact intelligence operations without needing a significant army, equipment, or means to directly attack the United States. Instead, they use open-source information along with data stolen from computer breaches to assemble a larger picture and understanding of past and possible future intelligence operations and tactical techniques and procedures (TTPs). With this compiled knowledge, adversaries will have a greater advantage and a higher chance of succeeding in compromising US intelligence operations in the future.

There is a high risk of exposure and targeting of US personnel with open and secret clearance by adversaries. This risk has increased significantly due to the abundance of foundational information that can be accessed through open-source methods. The biometric system at borders has been mentioned as an example of how countries that support terrorists may try to invade the protection system of another country to destabilize their agents and counterterrorism intelligence system.

OSINT, or Open Source Intelligence, is a way of gathering information that does not require the use of hacking or private credentials to access data. Simply viewing someone's public profile on social media is an example of OSINT. However, using someone's login information to access private information is not considered OSINT.

In the context of intelligence agencies, OSINT refers to information that is obtained from unclassified sources. If this information is combined and analyzed with data from a breach such as the OPM breach, then the adversary will have a significant advantage over US personnel.

An advantage of using a comprehensive approach to intelligence gathering is that each discipline is suited to collect a particular type of data. This allows intelligence organizations to examine all facets of an intelligence target and gain a better understanding of how it operates.

The aggregated information will also significantly improve the adversary's biometric technology detection program at border crossing points to identify the US-cleared personnel and therefore limit the effectiveness of intelligence operations in that country. The effects of OSINT and data breach materials, combined with biometric technology used at border crossings by adversaries to detect open and secret IC and DoD personnel, pose an ongoing threat for the foreseeable future. OSINT, the popular and easily searchable method, fell into disuse after World War II. Intelligence agencies focus on methods that use sophisticated tools to deal with the more glamorous and dangerous world of HUMINT. The application of new technologies has made border crossings safer for those in control, but more perilous for authorized personnel. These technologies are implemented to enhance security, improve convenience, and decrease waiting times at border checkpoints.

Furthermore, with the establishment of a new internal intelligence framework, we can effectively combat terrorism using the threat intelligence life cycle. The final output will vary based on the initial requirements for intelligence, including the information sources and target audience.

Threat Intelligence, or Cyber Threat Intelligence, is a discipline based on intelligence technics that aims to collect and organize all information related to threats in cyberspace, to draw up a portrait of attackers or to highlight trends.

This new counterterrorism structure will divide threat intelligence into three subcategories:

Strategic: intelligence is a type of intelligence that is reserved for general managers and/or presidents. It targets major issues and involves more predictive rather than reactive information. This type of intelligence results from simple information and in-depth analysis. Strategic intelligence explores long-term, far-reaching solutions and is different from tactical intelligence, which is more focused on short-term solutions. In short, tactical and strategic intelligence are opposites on the intelligence scale (Itai Shapira, 2020).

Tactical: intelligence is designed to answer a specific question. It is mainly produced for personnel working in the field who need intelligence in their day-to-day tasks. For instance, a counterintelligence screening officer who receives intelligence regarding allegations of espionage would benefit from tactical intelligence (Gómez, J. C., 1990)

Operational: intelligence will be generated for decision-makers and management to address general issues. This type of intelligence, which is both descriptive and predictive, results from a well-balanced combination of information and analysis.

Summary of the Study

The study's focus was on case studies as a means to highlight the benefits of a well-functioning intelligence cycle in the fight against terrorism at the domestic level of allied countries. It's important to keep in mind that domestic terrorism is solely perpetrated by local groups with no connections outside the United States. In contrast, international terrorists' activities tend to transcend national borders and are frequently backed by international entities.

The study also comments on how adversaries are using open source intelligence, data breach information, and biometric technology to negatively impact intelligence operations, as well as US personnel who support the anti-terrorism mission. The case studies were chosen for their ease of access to open source material, and to help understand whether any aspect of the intelligence operation or personnel has been affected by interference or conflicting exposure.

The text below is already clear and well-written. I cannot find any spelling, grammar or punctuation errors. However, I can rephrase it for you: The case studies analyzed the methods used by adversaries to affect intelligence operations, including the use of OSINT, information from data breaches, and biometric detection technology. Each case study was carefully examined and then compared to reveal their commonalities and shortcomings. The studies were then organized into a comparison matrix, assigning a value of either "1" or "0" to each attribute to illustrate their effectiveness against intelligence operations and US-cleared personnel. In addition, a comparative case study was presented, comparing countries with strong intelligence systems to those with weaker systems, including allies and weaker nations.

Discussion of the Findings

This study highlights cases of information leaks and the use of biometrics or the Internet, which present a risk not only for the country but also for its agents. When it comes to counterintelligence or counterterrorism, innocent human lives can be lost due to negligent operations carried out by agents of the intelligence community. This can sabotage the role of U.S. intelligence and prevent a better understanding of biometric technology that other countries have already implemented.

U.S. intelligence operations are vulnerable to adversaries due to the large amount of open-source intelligence (OSINT) information and data breaches available on the Internet. Biometric technology, which is rapidly advancing, is also being used to influence intelligence operations. When authorized U.S. personnel cross borders abroad, biometric scanning technology is used to intercept, expose, or identify them while conducting or supporting intelligence operations. The information that powers many of these biometric software databases comes from OSINT or even hacked documents, like the Office of Personnel Management's personal information in 2015

The phenomenon of open-source hardware theft has been sufficiently demonstrated, including stolen OPM hardware. This theft was most damaging to those who had security clearance and supported intelligence operations. Enemies of the United States who could penetrate the secret files could steal millions of SF-86 security clearance forms. These files were extremely valuable because they contained personal and other critical information already collected for each person. The consequence was very serious because the enemy could intercept the identified agents and blackmail them.

The enemy is increasingly able to use open-source material to obtain individuals' information from multiple websites. This poses a significant threat to intelligence operations, particularly in the case of adversaries who use open-source methods to expose CIA front companies, personnel, and aircraft linked to rendition operations. Such entities have been revealed through online court documents, bank documents, financial documents, phone calls, and incorporation documents found in state departments. The best use of open source has become a staple of enemies of the United States, enabling them to easily identify countless shell company names, PO Box addresses, office addresses, phone numbers, secret and overt identities, affiliates' legitimate bank accounts, aircraft tail numbers, and other supporting devices necessary to conduct these intelligence operations. As a result, these supporting devices have been permanently compromised by open-source means.

Rebuilding anti-theft capabilities would cost millions of dollars, but the greatest concern is the irreparable damage that the reputation of the United States would suffer in the eyes of the world. It is not just about the collateral sums to be disbursed to fight against information theft, nor the damage to care methods or even dismissed employees and their careers. Rather, the damage to the United States was discovered by journalists and reporters investigating initial reports of CIA planes and illegal kidnappings, such as the one carried out by the CIA in Milan, Italy. What is ultimately puzzling is the revelation of the entire rendition program that led the US government to reassess the program and shut down part of it under the Obama administration. It has been revealed that the CIA has been using their own planes and shell companies for their operations, which has been exposed to companies that operate their planes on their behalf. The details that have been revealed have led investigators to obtain intricate details of the 2003 abduction of Abu Omar by CIA agents in Milan, Italy.

The Italian investigators have utilized several open-source methods and digital forensics to reconstruct the kidnapping operation. The use of real names and the credit cards used in hotels have made it possible to spot CIA agents, who forgot to change their cell phone SIM cards. If the use of these coins had not been made, the whole operation could have been successful without these complacent actions and bad trades. Poor operational security and botched operational TTPs used by CIA agents allowed Italian investigators to rebuild most of their operations. The open-source research methodology has led adversaries to expose several CIA front companies, including the real identities of undercover agents, their mailing addresses, the number of aircraft tails, and other legitimate companies that have been compromised and can no longer do business with the CIA. The damage caused by these operations is related to the rendition, but the operations turned out to be catastrophic for the CIA, as the program was drastically reduced, and other elements were eliminated.

The assassination of the Israeli Mossad in Dubai was a significant intelligence operation that was compromised due to biometric technology. While many leading experts suspect that the Israeli Mossad was responsible for the mission, it has never been confirmed by the Israeli government. The primary objective of the mission was to assassinate Mahmoud Al-Mabouh and it was successful. However, investigators in Dubai were able to reconstruct the movements of suspected Israeli agents using biometrics and open-source information left behind. As a result, operational movements, identities, TTPs, shell companies, and other logistical support elements were exposed. This means that operatives who may have performed the mission previously will no longer be able to conduct espionage activities. Authorities in Dubai used CCTV cameras to investigate the murder of Al-Mabhouh (Goold, B. J. (2004).

They reconstructed the suspects' movements until they arrived at the airport, where the authorities were able to find their passports and photographs. Biometric detection technology was used at Dubai International Airport, which only collected copies of passports. No other data, such as fingerprints, iris scans, or facial recognition images, were collected from travelers.

Cases of biometric identity theft can be reported, but this requires a well-trained police force. During Abu Omar's kidnapping, the authorities were unable to verify the data available on the scanned copy of the passports used by Mossad agents. No other biometrics, such as retina or fingerprints, had been collected by border officials.

Shortly after the passport details were discovered, authorities in the United Arab Emirates quickly released the photographs and issued international arrest warrants. The Israeli operation got even more out of control and collapsed completely when authorities discovered that the names used in several passports belonged to real Israelis located in other countries. Essentially, the Mossad committed identity theft and passport fraud of real citizens and was caught red-handed and publicly embarrassed in the international media. While other intelligence operations have been embarrassing for their governments, this mission has received the most publicity in recent years.

Although the passport details were fake, the images in the documents were real. A fake passport is a counterfeit of a passport or other travel document issued by a country or authorized agency. These falsified passports can be used for various illegal activities like identity theft, age fabrication, illegal immigration, organized crime, and even by security agents. It is safe to assume that the UAE government probably entered photos of Mossad operatives into facial recognition software that it used with biometric scanning technology at the border.

It is also highly likely that the UAE has information exchange agreements with other countries in the region, and these countries may also have the same photographic evidence incorporated into their biometric detection systems. The use of biometrics could have serious implications for US-cleared personnel who operate undercover with a pseudonym or their real identity.

The following text discusses the limitations of using TTP passports due to the sensitive and classified nature of overseas activities. The researcher concluded that future operational activities using these passports will be limited as the Israeli government did not even accept responsibility for the Dubai assassination mission. Moreover, there is limited information available on the effectiveness of competing biometric technologies that compromise US cleared personnel and intelligence operations. This is due to the sensitive and classified nature of US intelligence activities.

Access to classified results from the intelligence community would have contributed or influenced the overall results of this study in several ways. For instance, accessing damage assessments typically conducted after a security breach or other FISS penetration against a mission or intelligence component would have helped incorporate those results into this study. Additionally, assessing what tactics, techniques, or procedures could have been adjusted after a mission was compromised would have been helpful. Finally, access to classified information would have revealed whether there were other recommended OPSEC procedures prior to an operational intelligence failure.

The report by the OPM Inspector General was highly valuable and timely for this study. However, there were no similar reports available to suggest adjustments to the underground TTPs after the OPM breach. The OPM data breach, which is believed to have been carried out by hackers associated with the Chinese government, resulted in a significant amount of material being stolen from US-cleared personnel, including the author's SF-86. It will take years to fully comprehend the impact of this breach on intelligence operations. The fact that the stolen OPM data was not made available on the Internet indicates that an adversarial government was most likely responsible for orchestrating the theft.

Implications for Practice

The harsh methods used by the American security and defense system have led to new tactics from terrorists, such as becoming lone wolves and leaving the US. As a result, these terrorists have moved to weaker allied countries of the US where they train new members and engage in illegal activities, all while waiting for an opportunity to attack American interests both within and outside the country's borders. This has created a dangerous situation that needs to be addressed.

Meanwhile, some of the allied countries, especially those in Africa, are becoming weary and turning to Russia for bilateral cooperation. The Russian government readily grants their requests, as they understand the United States' inability or lack of good faith towards these allies. North African countries, including Burkina Faso, Mali, Senegal, and Gabon, are seeking to rid themselves of French and American influence.

It is appropriate for the US government to take three steps to protect the effectiveness of future intelligence operations, given the damage caused by bad intelligence practices and the need to do better. The following are two actions that the US government must take to counter the damage caused by the OPM (Office of Personnel Management) violation:

Firstly, the creation of new supporting entities such as cover identities and front companies linked to those identities. These entities should have a significant transactional history and business activity, along with a meaningful social media presence and robust verifiable credentials. This step is necessary because any information lost by the OPM breach will most likely have a reference or connection to bogus organizations and secret figures used by US-cleared personnel in past or current intelligence operations. The counterintelligence gained from the OPM breach is a boon to the adversary who led it. Therefore, it will take decades to repair the damage done to leading figures and organizations used to conduct intelligence operations.

Secondly, the US government must hold adversaries accountable by directing and publishing cyber operations on the scale of those perpetrated by DoD (Department of Defense), CI (Counterintelligence), and US industry. It is possible that the DoD and IC (Intelligence Community) are already in the process of conducting significant offensive cyber operations, but their success must be made public to deter those who might consider cyber-attacks. The frequency of cyber-attacks against American interests will most likely increase if there is a perception that there will be no consequences or repercussions from the United States against those who commit these actions.

The third and final action: The US government should take important actions to address the security concerns surrounding the SF-86 application and protect any new SF-86 application by keeping it on a self-contained computer network that is not connected to the Internet. If the recordings had been stored in a network that was not connected to the Internet, adversaries would not have been able to remotely connect to the system and steal the data from thousands of miles away.

Unfortunately, the outdated networks have not been strengthened due to a lack of investment over the years. The OPM Inspector General's report had already made similar recommendations before the massive breach occurred, but these software and hardware upgrades were never implemented for unknown reasons.

Recommendations for Further Research

After evaluating the security challenges faced by allied countries in their fight against terrorism, a question arose regarding the need to establish a domestic counterterrorism structure in each of those countries. This was to ensure the security of both the United States and its allies. To address this, the author proposed a multidimensional security framework that takes into account the various categories and dimensions of security, threat domains, intensity of threats, and regional significance of threats. The framework was developed specifically for assessing U.S. allied countries, but it is expected to be useful beyond the region as a tool that comprehensively considers the security of both the United States and its allies.

The proposed intelligence structure for counterterrorism can be a valuable tool for managing terrorism in countries that are friendly to the United States. This would help reduce stress within the United States by protecting its interests both domestically and abroad.

The public needs to understand the impact of the massive breach of OPM data, which includes the personal information of cleared US personnel. However, this can only be assessed once the theft has occurred. In classified environments, likely, the US intelligence community has already determined how the stolen OPM information has affected intelligence operations and the people who support them.

To prevent data breaches, the United States of America should advise cleared personnel to take inventory of the information stored on their computers and in their files. All data should be backed up and destroyed before disposal, and employees should be trained on updated security procedures. Additionally, computer usage should be monitored and security software should be kept up to date.

Studies have shown that data breaches occur frequently, with hacking attacks being the most common cause. In many cases, opportunistic hackers exploit weak or lost passwords as a vulnerability. In 2020, there were 1,923 confirmed cases of violations (49%), and the total number of compromised cases exceeded 37 billion, which is a 141% increase compared to 2019.

One can understand the gravity of the infringement by simply examining the term "PII violation," which undermines the extent of damage that can be inflicted against the government. Such a breach of personal information involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any comparable situation where individuals other than those authorized to gain access to personally identifiable information for purposes other than those authorized.

It is important for the government to regularly conduct audits and change the passwords of the devices used to ensure cyber security. Changing passwords periodically is mandatory. Furthermore, it is crucial to identify and monitor hacking sites that attract individuals.

However, until this information is published in a declassified damage assessment, researchers in this field will have to be patient before establishing stronger correlations with endangered intelligence operations. Breaches of additional databases containing personally identifiable information (PII) will only continue to increase exponentially. Although industries such as hospitality have not yet suffered significant breaches, it is only a matter of time before a large hotel chain and its guest data are exposed, giving adversaries access to sensitive information that could compromise intelligence operations.

Biometric recognition technology presents both challenges and opportunities for wider implementation. Therefore, the United States should understand that these systems are complex and require immediate attention. Furthermore, biometric recognition is inherently probabilistic, and measures must be taken to accompany experts in using this technology.

To ensure the comprehensive assessment of biometric recognition, the US government needs to provide access to education for members of the intelligence community. This will enable them to master the topic in detail and provide policymakers, developers, and researchers with an in-depth understanding of the current capabilities, possibilities for the future, and the role of the government in technology and systems development.

Conclusion

All intelligence agencies must ensure that the information collected by their agents or agency is kept in secure locations without an internet connection to prevent any potential information breaches. The most significant threats are from hackers who specialize in stealing online information and sending viruses to destroy the systems of states they view as enemies. To counter these threats, a new intelligence structure must be established to focus on the fight against terrorism. This structure should prioritize maintaining the security of agents and the agency against these attacks. It is essential to conduct in-depth research on this issue and make the necessary efforts to address it.

The digital age has brought about various risks, as critical information is stored on computers that are connected to the open internet. The US government must prioritize the protection of its agents and allied countries' agents against cybersecurity threats since the success of intelligence operations depends on the US-cleared personnel supporting them.

The Department of Defense and Intelligence Community has learned a hard lesson from the OPM breach, which resulted in a catastrophic loss of data. This breach has permanently affected generations of intelligence officers who have worked in the past, in ways that are beyond their control. Many of them won't be able to travel to certain countries where they previously operated under pseudonyms of identity.

Due to the negligence and mistakes in data protection, several members of the intelligence community, who have close friends, family, and associates overseas, have also been permanently affected. The loss of information by OPM will have significant ramifications on the US-cleared personnel and the intelligence operations they have supported for decades.

Cybercrime is a growing concern for the protection of national security operations and the information of US-cleared personnel. To ensure data security, it is crucial to store this sensitive information more securely. The frequency of cyber-attacks is only expected to rise, making data protection even more important. The US government has a responsibility to safeguard this critical information and must learn from past data theft case studies, such as the OPM breach, to strengthen their unclassified networks. One of the technologies used by several companies for security purposes is Suprema, a biometric locking system. However, it is important to understand the risks associated with using biometrics and fingerprints. Criminals can use fingerprints and facial recognition to gain access to secure facilities in the same way that businesses use them to authorize employee access. Security experts believe that the database of BioStar, which uses Suprema, was unprotected, allowing someone to gain access and potentially steal the information.

This study aims to explain the risks associated with a biometric data breach. Biometric information, such as fingerprints, retina, face, or voice, is part of an individual's identity and cannot be changed like a password. When cybercriminals gain access to biometric data, they gain access to information that can be linked to an individual's identity forever. Biometric data is used in buildings for security purposes, where individuals use it to gain access. However, cybercriminals can misuse this data by stealing an individual's fingerprints, potentially damaging their reputation and stealing valuable information. While biometric data may not be useful to open a credit account, it has other applications such as boarding an aircraft. The number of applications for biometric data will likely increase in the future. The United States may need to consider older methods of securing information instead of relying on advanced technology.

The Federal Guard Service, responsible for protecting Russian President Vladimir Putin and overseeing secure communications for the Kremlin, invited companies to bid on a contract for typewriters and paper carbon made in Germany in 2013. Nikolai Kovalev, former director of the Russian Federal Security Service, stated that electronic communication is vulnerable from a security perspective, and primitive methods such as a person's hand and a pen, or a typewriter are preferable for keeping secrets. Mr. Kovalev's statement was in response to operational intelligence posted on WikiLeaks, which revealed that UK-based US spies had intercepted top-secret communications from then-Russian President Dmitry Medvedev during his visit to Britain for the G20 summit in London in 2009. The National Security Agency (NSA), an American surveillance and eavesdropping organization that shares information with senior officials in Britain, Australia, Canada, and New Zealand, prepared a briefing that laid out the details of the interception

It is essential to address the wiretapping incident that happened in 2009, which involved espionage and the revelation of a document written four months after President Medvedev visited London. At that time, the NSA intercepted communications from the Russian delegation. To prevent cybercrime attacks in the future, the US must think outside the box and learn from past incidents. The exposure of such information could lead to spear-phishing emails, which can grant access to computer systems. Regarding China's data theft, the US should be concerned about how the information obtained from OPM breaches may be used. The Chinese government could create a vast database of federal employees to identify US officials and their roles. This could compromise the security of authorized agents, leading to the loss of future missions. Therefore, it is crucial to protect the image of the United States and all members of the intelligence community

References

Aljohani, Abeer. (2023). "Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility" Sustainability 15, no. 20: 15088. https://doi.org/10.3390/su152015088

Aly, H. (2022), "Digital transformation, development and productivity in developing countries: is artificial intelligence a curse or a blessing?", Review of Economics and Political Science, Vol. 7 No. 4, pp. 238-256. https://doi.org/10.1108/REPS-11-2019-0145

Andrew, (2001) 'Intelligence, InternationalRelations', pp. 29–41. For recent research on signals intelligence, see Matthew Aid and Cees Wiebes (eds), Secrets of Signals Intelligence during the Cold War and Beyond, Special Issue of Intelligence and National Security, 16/1(2001).

Andrew Owen Bennett and George Alexander L. George (2007) Case Studies And Theory Development In The Social Sciences. March 2007 Perspectives on Politics 5(01):256 DOI:10.1017/S1537592707070491 Edition: 1st Ed.Publisher: MIT Press

Andrew Silke (2019): The Routledge Handbook of Terrorism and Counterterrorism. Abingdon, Oxon: Routledge

Andrienko, Gennady, Natalia Andrienko, and Stefan Wrobel. 2007. "*Visual Analytics Tools for Analysis of Movement Data."* ACM SIGKDD Explorations Newsletter. doi:10.1145/1345448.1345455.

Artiga, Vic (2010), 'Lone Wolf Terrorism What We Need to Know and What We Need to Do', September 14-16, 2010, cf: http://www.takresponse.com/index/homelan d-security/lone-wolf_terrorism.html.

Bakker, E. (2012). Forecasting Terrorism: The Need for a More Systematic Approach. *Journal of Strategic Security*, *5*(4), 69–84. http://www.jstor.org/stable/26463974

Basu N. (2021). Learning Lessons from Countering Terrorism: the UK Experience 2017–2020. Cambridge Journal of Evidence-Based Policing, 5(3-4), 134–145. https://doi.org/10.1007/s41887-021-00068-1

Beam, Louis,(1992), Leaderless Resistance', The Seditionist, Issue 12, 1992, cf: http://www.louisbeam.com/leaderless.htm

Bennett, Brian, & Hennigan, W.J. 2015, September 16. China and Russia Are Using Hacked Data to Target U.S. Spies, *Officials Say*.. http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html

Bennie G. Thompson (2006 p. 6). “The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy,” University of Pittsburgh Journal of Technology Law & Policy, Spring 2006

Berman, Emily (2016) "The Two Faces of the Foreign Intelligence Surveillance Court," Indiana Law Journal: Vol. 91: Iss. 4, Article 4.
Available at: https://www.repository.law.indiana.edu/ilj/vol91/iss4/4

Boaz Ganor (2005): The Counter-Terrorism Puzzle: A Guide for Decision Makers. New Brunswick, NJ: Transaction Publishers

Botha Jennifer. 2015 & 2016. Global Data Breaches Responsible for the Disclosure of Personal Information: https://core.ac.uk/download/pdf/231923014.pdf

Bonelli, L. (2023). Chapitre 9. Renseignement intérieur et antiterrorisme en France. Dans : Jacques de Maillard éd., Police et société en France (pp. 199-220). Paris: Presses de Sciences Po. https://doi.org/10.3917/scpo.maill.2023.01.0199

Bureau of Counterterrorism (2001). Foreign Terrorist Organizations (FTOs). Terrorist Designations and State Sponsors of Terrorism. Retrievable at https://www.state.gov/foreign-terrorist-organizations/

Burnett, Jonny and Whyte, Dave. 2005. “Embedded expertise and the new terrorism,” Journal for Crime, Conflict and the Media, Volume 1, Issue 4. 1-18.

Brannen, Kathleen. April 6, 2015. To Catch a Spy. Biometrics is Making It Far More Difficult for The U.S. Intelligence Community to Conduct Clandestine Operations. http://foreignpolicy.com/2015/04/06/to-catch-a-spy-biometricscia-border-security/

Brian Michael Jenkins (2021), “Op-Ed: Why we need a Jan. 6 Commission to investigate the attack on the Capitol,” Los Angeles Times, January 19, 2021, https://www.latimes.com/opinion/story/2021-01-19/jan-6-commission-capitol-attacks.

Byman, Daniel (2007):”US Counter-terrorism Options: A Taxonomy”. Survival 49, no. 3, pp. 121-150.

Claudia Grisales (2021), “New Jan. 6 Report Describes Intel Failures And The Warnings Police Got In December, NPR, June 8, 2021, https://www.npr.org/2021/06/08/1004493986/new-jan-6-report-describes-intel-failures-and-the-warnings-police-got-in-decembe

Clemons, Steve (2010), ‘The Real Problem with “Lone Wolf” Terrorism”, 20 April 2010, cf: http://www.thewashingtonnote.com/archives /2010/04/the_real_proble

Christopher Andrew, (2000), ‘Intelligence in the Cold War: Lessons and Learning’, in Harold Shukman(ed.), Agents for Change: Intelligence Services in the 21st Century (London: St Ermin’s Press 2000), pp.1–2.

Christopher Andrew, (2004) ‘Intelligence, International Relations and ‘‘Under-theorisation’’’, this volume, pp.29–30.

Christopher Andrew, (1995) For an excellent analysis of presidents and their use of intelligence. For the President’s Eyes Only: Secret Intelligence and American Presidency from Washington to Bush (London: Harper Collins1995).

Christopher Andrew and David Dilks (1984), The Missing Dimension: Governments and Intelligence Communities in the 20th Century (Urbana, IL: University of Illinois Press 1984).

Christopher R Moran, Joe Burton, George Christou (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying, Journal of Global Security Studies, Volume 8, Issue 2, June 2023, ogad005, https://doi.org/10.1093/jogss/ogad005

Chopin, O. & Oudet, B. (2023). Chapter 2. The intelligence cycle. In: O. Chopin & B. Oudet (Dir), Intelligence and Security (pp. 53-73). Paris: Armand Colin.

Clint Watts et William McCants (2016). « What is the future of al-Qaida and the Islamic State? (part 2) », Experts Weigh In (Brookings), n° 24 (28 janvier 2016), p. 2, http://www.brookings.edu/blogs/markaz/posts/2016/01/28-experts-weigh-in-al-qaida-isis-watts-mccants;

Constantin LOPM. 2015, July 30. Anthem Hackers Reportedly Also Breached United Airlines. http://www.pcworld.com/article/2954872/opm-anthemhackers-reportedly-also-breached-united-airlines.html

COT (ed.2007), Lone-Wolf Terrorism. Case study for Work Package 3 'Citizens and governance in a knowledge-based society', TTSRL, July 2007, cf: http://www.transnationalterrorism.eu/tekst/publications/Lone-Wolf%20Terrorism.pdf

Crenshaw, M. (Ed.). (2010). The Consequences of Counterterrorism. Russell Sage Foundation. http://www.jstor.org/stable/10.7758/9781610447287

Dixon, A. L., Gassenheimer, J. B., & Barr, T. F. (2003). Identifying the Lone Wolf: A Team Perspective. The Journal of Personal Selling and Sales Management, 23(3), 205–219. http://www.jstor.org/stable/40471921

Donadio, Renato. November 4, 2009. Italy Convicts 23 Americans for C.I.A. Renditions. http://www.nytimes.com/2009/11/05/world/europe/05italy.html

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. The Academy of Management Review, 14(4), 532–550. https://doi.org/10.2307/258557

Farmer, B. British Spies Trawl Ashley Madison Leak for Intelligence. August 31, 2015. http://www.telegraph.co.uk/news/uknews/defence/11830594/ British-spies-trawl-Ashley-Madison-leak-for-intelligence.html

Fantz, Ashley. March 23, 2015. As ISIS Threats Online Persist, Military Families rethink Online Lives. http://www.cnn.com/2015/03/23/us/online-threatisis-us-troops

Federal Trade Commission Act of (2006) Competition Consumer Protection Law 15 U.S.C. §§ 41-58, as amended. http://uscode.house.gov/view.xhtml

Flanagan, S. J. (1985). Managing the Intelligence Community. International Security, 10(1), 58–95. https://doi.org/10.2307/2538790

Finklea, K. 2015. Cyber Intrusion into U.S. Office of Personnel Management: In Brief (CRS Report No. R44111). Washington, DC: Congressional Research Service.

Finley, C. J. (2015), Terrorism and the Right to Resist: A Theory of Just Revolutionary War, Cambridge: Cambridge University Press

Finn, Patrick, & Tate, John. 2011, August 31. N.Y. Billing dispute Reveals Details of Secret CIA Rendition Flights. https://www.washingtonpost.com/world/ national-security/ny-billing-dispute-reveals-details-of-secret-cia renditionflights/2011/08/30/gIQAbggXsJ_story.html

Fisher, Daren G., and Laura Dugan(2019) 'Sociological and Criminological Explanations of Terrorism', in Erica Chenoweth, and others (eds), The Oxford Handbook of Terrorism, Oxford Handbooks (2019; online edn, Oxford Academic, 4 Apr. 2019), https://doi.org/10.1093/oxfordhb/9780198732914.013.10, accessed 30 Jan. 2024.

Franck Bulinge and Éric Boutin, (2015). "Intelligence as an object of research in SHS: the central role of CIS", Communication et organization, 47 | 2015, posted online June 1, 2018, accessed December 24, 2023. URL: http://journals.openedition.org/communicationorganization/4951; DOI: https://doi.org/10.4000/communicationorganization.4951

Fred Burton and Stewart, Scott, (2008) 'The Lone Wolf Disconnect', 30 January 2008, Stratfor, cf: http://www.stratfor.com/weekly/lone_wolf_di sconnect

Ganor, B. (2002), 'Defining Terrorism: Is One Man's Terrorist Another Man' Freedom Fighter?', Police Practice and Research: An International Journal, 3(4), pp. 287-304

Garrett Pierman (2015). « The Grand Strategy of Nonstate Actors: Theory and Implications », Journal of Strategic Security 8, n° 4 (hiver 2015), p. 76, http://search.proquest.com/docview/1753045155?accountid=9867.

Gerring, John 2001) Social Science Methodology: A Criterial Framework. New York: Cambridge University Press, 2001.)

Gill, Peter, and Mark Phythian (2006). Intelligence in an Insecure World. Malden, MA: Polity Press, 2006.

Hannas, Chad, Mulvenon, James. and Pugli, A.B. 2014. Chinese Industrial Espionage: *Technology Acquisition and Military Modernization.* Foreign Affairs, 210-215.

Hamm, Mark (2002), In Bad Company. America's Terrorist Underground, Northeastern University Press, 2002.

Herman (1993), Intelligence Power, and Abram Shulsky, Silent Warfare: Understanding the World of Intelligence (London: Brassey's US 1993).

Hendricks, Steve .2010. A Kidnapping in Milan: The CIA on Trial. NY: W.W. Norton & Co. n°

Henry Laurens (2011/2), Metropolises and colonial empires, Le Débat 2011/2164), pg70 to 84, Posted online on Cairn.info on 04/29/2011, https://doi.org/10.3917/deba.164.0070

Herridge, C., & Dean, Michael. 2015, September 16. China reportedly compiling 'Facebook' of U.S. government employees. http://www.foxnews.com/politics/ 2015/09/16/chinas-facebook-us-government-employees/

Hewitt, Christopher (2003), Understanding Terrorism in America. From the Klan to al Qaeda, London, and New York: Routledge 2003.

Hiltzik, Michael. 2015, March 6. *Anthem is Warning Consumers About Its Huge Data Breach*. Here's a Translation. http://www.latimes.com/ business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html

Hobart, P. M. (2008). Domestic Intelligence: Functions and Form: Some Thoughts, Ideas and Recommendations. *American Intelligence Journal*, *26*(1), 8–17. http://www.jstor.org/stable/44327209

Hoffman, A. M., & Shelby, W. (2017). When the "Laws of Fear" Do Not Apply: Effective Counterterrorism and the Sense of Security from Terrorism. Political Research Quarterly, 70(3), 618–631. http://www.jstor.org/stable/26384928

Itai Shapira (2020) Strategic intelligence as an art and a science: creating and using conceptual frameworks, Intelligence and National Security, 35:2, 283-299, DOI: 10.1080/02684527.2019.1681135

Gill, P. and Phythian, M. 2006. Intelligence in an Insecure World, Cambridge: Polity.Goldman, J. (ed.) 2006, Ethics of Spying: a reader for the intelligence professional. Lanham, MD: Scarecrow Press

Gómez, J. C. (1990). Primate tactical deception and sensorimotor social intelligence. Behavioral and Brain Sciences, 13(2), 414–415. doi:10.1017/S0140525X00079516

Goold, B. J. (2004). CCTV and policing: Public area surveillance and police practices in Britain. Clarendon Studies in Criminology.

Gray, Stephen. 2006. *Ghost Plane*: The True Story of the CIA Torture Program. New York, NY: St. Martin's Press.

James J. F. Forest (2015): Essentials of Counterterrorism. Santa Barbara: ABC-CLIO.

Jamal, Amaney. and Naber, Nadine. Eds. 2008. Race and Arab Americans Before and After 9/11: from Invisible Citizens to Visible Subjects. Syracuse: Syracuse University Press.

John Ferris, R.Boyce and J.Maiolo (2003) 'Intelligence, The Origins of World War Two: The Debate Continues (Basingstoke: Palgrave 2003), p.308.

John Gerring, 2001) Social Science Methodology: A Criterial Framework (New York: Cambridge University Press, 2001, 219)

Johnson Joseph. 2021. Worldwide digital population as of January 2021 Published by Joseph Johnson Apr 7, 2021

Kaplan, Jeffrey, (1997) Leaderless Resistance, Terrorism and Political Violence, vol. 9 (1997), no. 3, pp.80-95.

Karoun Demirjian (2021), "Momentum of Capitol riot inquiries stalls amid partisan flare-ups," Washington Post, March 16, 2021, https://www.washingtonpost.com/national-security/capitol-riot-congressional-inquiries/2021/03/16/a667c1ac-85ca-11eb-82bc-e58213caa38e_story.html.

Kenneth Udokporo, C., 2021). Understanding the Stages of the Product Life Cycle. IntechOpen. doi: 10.5772/intechopen.99036.

Kott Matthew (2018). British intelligence, and Hitler's empire in the Soviet Union, 1941–1945 J. Baltic Stud., 49 (2) pp. 268-271, 10.1080/01629778.2018.1469843

Kowsmann, Patricia. October 8, 2015. Ex-CIA Agent Detained in Portugal Over 2009 Kidnapping Conviction in Italy., http://www.wsj.com/articles/excia-agent-detained-in-portugal-over-2009-kidnapping-conviction-in-italy1444324821

Kushner, H.W., (2003) Encyclopedia of Terrorism, Thousand Oaks and London: pp.144-5; Hewitt, 2003: p.79 Sage 2003.

Lee, Gomes (2001). That thicket of hair just spoils the view of all those muscles. *Wall Street Journal*, 5 September, A1-A1

Len Scott & Peter Jackson (2004) The Study of Intelligence in Theory and Practice, Intelligence & National Security, 19:2, 139-169, DOI: 10.1080/0268452042000302930

Lewal J. (1881), War studies: Intelligence tactics, Paris, Baudoin, 1881, 2 volumes, republished in 2010 by Bibliobazaar.

Lewis-Beck, M., Bryman, A. E., & Liao, T. F. (2003). The Sage encyclopedia of social science research methods. Los Angeles, CA: Sage.

Loch K. Johnson (1983), "Seven Sins of Strategic Intelligence," World Affairs, 146, no. 2 (1983): 176–204, https://www.jstor.org/stable/pdf/20671981.pdf;

Lord, Jonathan. 2015. Undercover Under Threat: Cover Identity, Clandestine Activity, and Covert Action in the Digital Age. *International Journal of Intelligence and Counterintelligence*, 28:4, 666-691, DOI: 10.1080/08850607.2015.1022464.

Lowenthal, Mark M. (2015) Intelligence: From Secrets to Policy. 6th ed. Thousand Oaks, CA: CQ Press, 2015.

Lowenthal Mark M. (2015), Intelligence: From Secrets to Policy, 6th ed. Thousand Oaks, CA: CQ Press, 2015, 297–312;

Mandel, D. R. (2003). Counterfactuals, emotion, and context. Cognition and Emotion, 17, 139-159.

Martha Crenshaw and Gary LaFree (2017): Countering Terrorism. Washington, DC: Brookings Institution Press.

Matthes, J., Schmuck, D., & von Sikorski, C. (2019). Terror, Terror Everywhere? How Terrorism News Shape Support for Anti-Muslim Policies as a Function of Perceived Threat Severity and Controllability. Political Psychology, 40(5), 935–951. http://www.jstor.org/stable/45204099

Martin, Aaron & Whitley, Edgar. (2013). Fixing identity? Biometrics and the tensions of material practices. Media, Culture & Society. 35. 52-60. 10.1177/0163443712464558.

Michael Herman (1998)' Diplomacy and Intelligence', Diplomacy & Statecraft, 9/2 (1998), pp.12.

Mintzberg, H. (1979). The structuring of organizations: a synthesis of the research. Englewood Cliffs, N.J. Prentice-Hall, 1979

Monica Czwarno (2006), "Misjudging Islamic Terrorism: The Academic Community's Failure to Predict 9/11," Studies in Conflict and Terrorism 29:7 (October–November 2006): 657.

Nathan Lean (2012). The Islamophobia Industry: How the Right Manufactures Fear of Muslims. Pluto Press. 2012. 222 p.

National Commission on Terrorist Attacks upon the United States, (2003). The 9/11 Commission Report (New York: W.W. Norton & Company, 2003), 353. The inability to manage and fuse foreign and domestic intelligence information was identified as a key shortfall.

National Commission on Terrorist Attacks Upon the United States, (2004). The 9/11 Commission Report, Washington, DC: July 22, 2004, hereafter referred to as the 9/11 Commission Report.

Nicolas Beau, Olivier Toscer (2019) In the eye of the RG, Intelligence category. Ed. Robert Laffont 03/10/2019, p. 245, EAN: 9782221220818

Peterson, Adrian. July 29, 2015. *What Would Chinese Hackers Want to Go After an Airline?* https://www.washingtonpost.com/news/the-switch/wp/2015/ 07/29/why-would-chinese-hackers-would-want-to-go-after-an-airline/

Phythian, M. (2009). The British Intelligence Services. In: Jäger, T., Daun, A. (eds) Geheimdienste in Europa. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91491-6_1

Pomerantz, SL(1987) FBI Law Enforcement Bulletin Volume: 56 Issue: 11 Dated: special issue (October 1987) Pages: 14-17 NCJ Number 107703. Retrievable at https://www.ojp.gov/ncjrs/virtual-library/abstracts/fbi-and-terrorism

Pune, Maharashtra. 2020. Open Source Intelligence (OSINT). Market Research Report-Global Forecast to 2023—*Market Analysis, Scope, Stake, Progress, Trends and Forecast to 2023*. Market Research Future. Available online: https://www.marketresearchfuture.com/reports/open-source-intelligence-market-4545 (accessed on 28 May 2020).

Rachael Levy and Siobhan Hughes, (2021) “Security Officials Blame Poor Intel for Failure to Blunt Capitol Attack,” Wall Street Journal, February 23, 2021, https://www.wsj.com/articles/top-security-officials-to-testify-on-failure-to-blunt-capitol-attack-11614084412.

Rao, Ursula. and Graham William Greenleaf. 2013. Subverting ID from above and below: *The uncertain shaping of India’s new instrument of e-governance, Surveillance and Society*, 11(3), pp. 287–300. doi: 10.24908/ss.v11i3.4496

Rathee, G., Maheswar, R., Sehar, S. et al. (2023). Towards reliable IoT communication and robust security: investigating trusted schemes in the internet of medical things using blockchain. Sci Rep 13, 20671 (2023). https://doi.org/10.1038/s41598-023-47989-7

Raymond L. Garthoff (2004); Foreign Intelligence and the Historiography of the Cold War. Journal of Cold War Studies 2004; 6 (2): 21–56. doi: https://doi.org/10.1162/152039704773254759

Richard K. Betts (2007), Enemies of Intelligence: Knowledge and Power in American National Security (New York: Columbia University Press, 2007), 9–14;

Robert J. Art and Louise Richardson (2007): Democracy and Counterterrorism: Lessons from the Past. Washington DC, USIP Press.

Roberts, K., & Herrington, V. (2010). Applying theory to intelligence practice: counter-terrorism and the psychology of small group development. Journal of the Australian Institute of Professional Intelligence Officers, 18(2), 43-55.

Roberta Wohlstetter, (1962) Pearl Harbor: Warning and Decision (Palo Alto, CA: Stanford University Press 1962).

Rohini Kurup and Benjamin Wittes (2021), “Was Jan. 6 an Intelligence Failure, a Police. Failure or Both?” and William Ford and Rohinia Kurup, “What Did We Learn From House and Senate Hearings on the Capitol Assault?” Lawfare, March 25, 2021, https://www.lawfareblog.com/what-did-we-learn-house-and-senate-hearings-capitol-assault.

Romanosky, S., Sharp, R., & Acquisti, A. (2010). Data breaches and identity theft: When is mandatory disclosure optimal? Paper presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard University, Cambridge, MA.

Ryan Goodman and Justin Hendrix, (2021) “January 6 Clearinghouse: Congressional Hearings, Government Documents, Court Cases, Academic Research,” Just Security, November 18, 2021, https://www.justsecurity.org/77022/january-6-clearinghouse

Ryan, Thomas. 2009. Getting in Bed with Robin Sage. Las Vegas, NV: Provide Security, LLC.

Schmid, A. P., Forest, J. J. F., & Lowe, T. (2021). Counter-Terrorism Studies: A Glimpse at the Current State of Research (2020/2021): Results from a Questionnaire Sent to Scholars and (Former) CT Practitioners. *Perspectives on Terrorism*, *15*(4), 155–183. https://www.jstor.org/stable/27044241

ShermanKent, (1949). Strategic Intelligence for American World Policy (Princeton, NJ: Princeton University Press 1949).

S/RES/1373, adopted on 28 September 2001.

Sullivan, J.P. and Lester, G. (2022). Revisiting domestic intelligence. Journal of Strategic Security, 15(1), 75-105. https://www.jstor.org/stable/48652012

U.S. Department of the Army. (2014 September 26). *Operations Security.* Army Regulation 530-1. Washington, DC: U.S. Department of the Army.

United States Government (1946). Hearings before the Joint Committee to Investigate the Attack on Pearl Harbor, 79th Congress 39 flights (Washington, DC: United States Government Printing Office 1946).

Venture Beat. 2020. US Homeland Security has used facial recognition on over 43.7 million people, *the machine Making sense of AI*. 6 February 2020. https://venturebeat.com/2020/02/06/u-s-homeland-security-has-used-facial-recognition-on-over-43-7-million-people/

William McCants and Clint Watts (2016) What is the future of al-Qaida and the Islamic State? Terrorism & Extremism Middle East & North Africa January 28, 2016

Worth, Kaite. 2016. “Lone Wolf Attacks Are Becoming More Common—And More Deadly.” FRONTLINE. July 14, 2016. http://www.pbs.org/wgbh/frontline/ article/lone-wolf-attacks-are-becoming-more-common-and-more-deadly/.

Ye, Qiang, Rob Law, Bin Gu, and Wei Chen. 2011. "The Influence of User-Generated Content on Traveler Behavior: *An Empirical Investigation on the Effects of E-Wordof-Mouth to Hotel Online Bookings*." Computers in Human Behavior 27 (2): 634–639. doi:10.1016/j.chb.2010.04.014.

Yin, R. K. (2017). Case study research and applications: Design and methods. Los Angeles, CA: Sage.

Youssef, Nagy. 2015. '*ISIS Hackers' Googled Their Hit List; Troops' Names Were Already on Public Websites*, March 23, 2015. http://www.thedailybeast.com/ articles/2015/03/23/isis-hackers-googled-their-hit-list-troops-names-were-alreadyon-public-websites.html

Zegart, A. B. (2005). September 11 and the Adaptation Failure of U.S. Intelligence Agencies. International Security, 29(4), 78–111. http://www.jstor.org/stable/4137498

APPENDICES

Physical and behavioral identifiers for biometrics authentication

This study delved into the significance of defining biometrics, by discussing the various types of biometrics utilized and highlighting the potential of biometrics in making authentication faster, easier, and more secure than traditional passwords. Although biometrics is a source of controversy, it nevertheless has the potential to revolutionize the authentication process.

Biometrics definition

Biometrics is a feature on devices that uses human physical or behavioral characteristics to identify individuals and grant access to systems, devices, or data. These biometric identifiers are unique to each person and can be used together to ensure greater identification accuracy. For example, a computer can be unlocked when it recognizes the fingerprint of an approved user. Assistance systems can automatically extract relevant information when they recognize the voice of an authorized person who has been identified in biometric authentication systems. Credentials, such as fingerprint scans and voice recordings, can be stored on devices, servers, or software used to scan them. However, facial recognition systems may face difficulty in recognizing users who wear makeup or glasses, or who are sick or tired. Similarly, variations in voice can also create confusion for biometric readings. Fingerprints and retinal scans are immutable, meaning they cannot be changed, and disclosing this biometric information could put users at permanent risk. From a legal standpoint, revealing biometric information can create significant legal exposure for the company that disclosed the data.

Types of biometrics

A biometric identifier is linked to intrinsic human characteristics divided into two categories which are: physical identifiers, as immutable and independent of the device, and behavioral identifiers. Fingerprints, facial patterns, voice or typing rate are well known by the public

1. Physical Identifiers

Fingerprints: Fingerprint scanners have become ubiquitous. Any touch device: a phone screen, mouse, or door panel has the potential to become an easy and convenient fingerprint scanner.

Photo and video: Any device equipped with a camera, can be used for authentication. Facial recognition and retinal scans are two common approaches.

Physiological recognition: Facial recognition is the second most common type of authentication. Other image-based authentication methods include hand geometry recognition, iris or retina scanning, palm vein recognition, and ear recognition.

Voice: Digital voice assistants and telephone service portals use speech recognition to identify authorized users and authenticate clients.

Signature: Digital signature scanners are widely used in retail checkouts and banks and users and customers already expect to be required to sign their name.

DNA: DNA scans are used by law enforcement to identify suspects. In practice, DNA sequencing has been too slow for widespread use.

2. Behavioral identifiers

Behavioral identifiers: Behavioral identifiers are a newer approach and are usually used alongside another method due to their lower reliability. These identifiers can become crucial, as they differ from physical identifiers, which are limited to a fixed set of human characteristics. In contrast, the only limit to behavioral identifiers is the human imagination. This approach is useful for distinguishing between a human and a robot. Here are some common approaches:

Typing patterns: Everyone has a different typing style when it comes to the speed at which they type, the time spent between letters, and the degree of impact on the keyboard.

Physical movements: The way people walk are unique and can be used to authenticate individuals in a building, or as a secondary layer of authentication for particularly sensitive locations.

Navigation patterns: Mouse movements and finger movements on trackpads or touch screens are unique to individuals and relatively easy to detect with software, no additional hardware is required.

Engagement patterns: With the help of technology, we can interact with each other in once-impossible ways. Our behavior can be analyzed and studied based on our usage patterns and habits. The way we open apps and use different locations can also be studied to identify us. Other factors that can be used to identify us include the times of day when we are most likely to use our devices, the way we navigate websites, the angle at which we hold our phones, and how often we check our social media accounts.