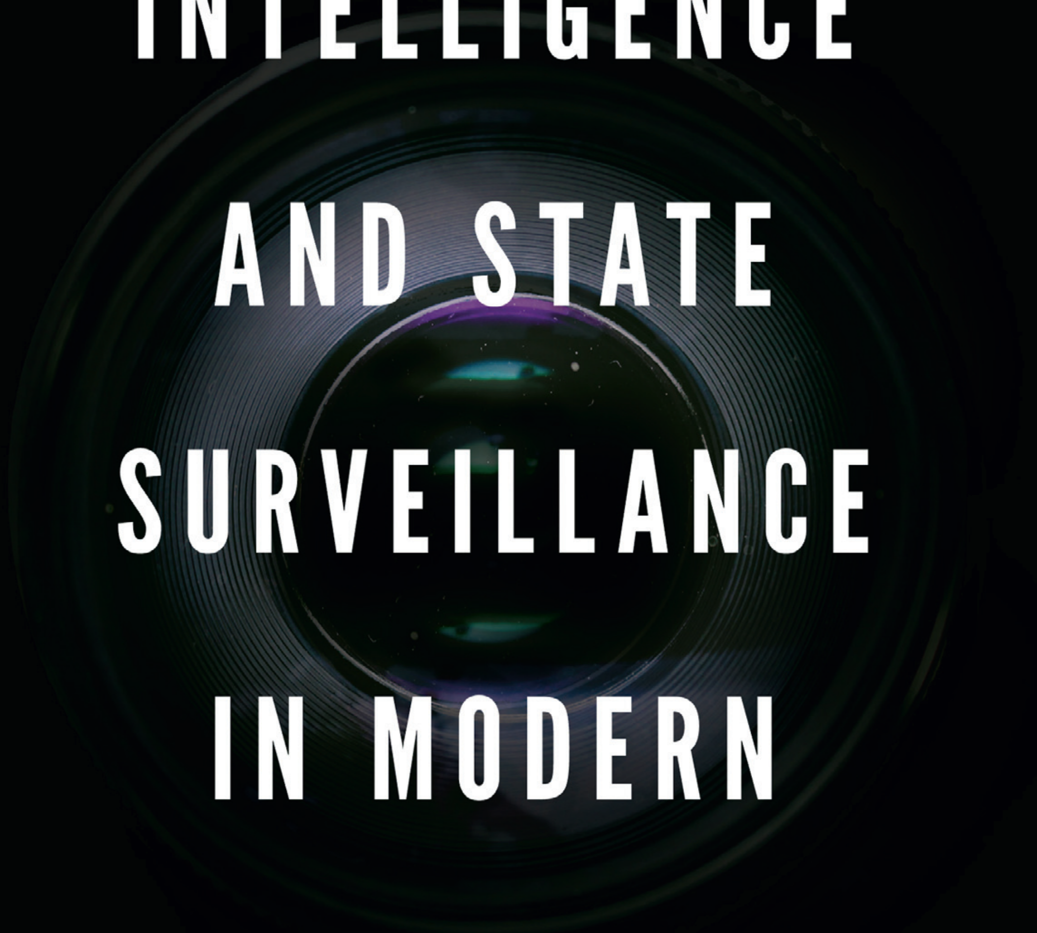
FREDERIC LEMIEUX

INTELLIGENCE AND STATE SURVEILLANCE IN MODERN SOCIETIES



AN INTERNATIONAL PERSPECTIVE

INTELLIGENCE AND STATE SURVEILLANCE IN MODERN SOCIETIES

This page intentionally left blank

INTELLIGENCE AND STATE SURVEILLANCE IN MODERN SOCIETIES: AN INTERNATIONAL PERSPECTIVE

BY

FREDERIC LEMIEUX

Georgetown University, USA

emerald
PUBLISHING

United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2019

Reprints and permissions service
Contact: permissions@emeraldinsight.com

No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a licence permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the chapters are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the chapters' suitability and application and disclaims any warranties, express or implied, to their use.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-78769-172-8 (Print)
ISBN: 978-1-78769-171-1 (Online)
ISBN: 978-1-78769-173-5 (Epub)

ISOQAR
REGISTERED
Certificate Number 1985
ISO 14001

ISOQAR certified
Management System,
awarded to Emerald
for adherence to
Environmental
standard
ISO 14001:2004.

INVESTOR IN PEOPLE

To Ophelia and Rose-Lynn… Never forget that true happiness does not come from without, it comes from within you.

This page intentionally left blank

Table of Contents

This page intentionally left blank

List of Figures

Introduction

Chapter 1

Chapter 3

Chapter 4

Chapter 7

This page intentionally left blank

List of Tables

Introduction

Chapter 2

Chapter 4

Chapter 6

Chapter 7

Chapter 9

This page intentionally left blank

Foreword

For several years, I have been contemplating writing a book that addresses current and emerging issues related to intelligence agencies and surveillance activities in modern societies after the fall of the Soviet Union in 1991. This contemplation was triggered and perpetuated by the multiple political, social, and financial events that occurred following the collapse of the Soviet Union, an event in and of itself, which certainly shaped and redefined the notions of threats and security on a global scale. Among these defining occurrences, I include Operation Desert Storm (1991), which was the first high-tech war necessitating a vast amount of real-time information to guide both missiles and ground troops toward their objectives. Due to these real-time technological capabilities, the United States–led coalition was able to free Kuwait from the Iraqi invasion in about one week. There are a myriad of other important engagements that demonstrate how Western military operations were guided and enhanced by various satellite surveillance and intelligence activities. The counteracting of transnational threats such as nonstate-sponsored terrorist groups in the Middle East (al-Qaeda and ISIL), the participation in burgeoning conflicts around the world including Eastern Europe (Serbia, Bosnia, and Herzegovina), and the monitoring of civil wars in Africa (Somalia) all were carried out with the aid of recent technological advances in intelligence and surveillance.

During the 1990s, knowledge of key technologies used and developed for military purposes were transferred to civilian institutions, most importantly the law enforcement agencies. Information technology hardware and software became available to police organizations to better manage crime and other domestic risks. This decade witnessed a rapid growth of computerization and information digitalization in the criminal justice system in general. These technological advances became mission critical to many police organizations, provoking structural and operational transformations such as centralization of information and adoption of new managerial models based on performance as well as data-driven security strategies.

The terrorist attacks of September 11, 2001 were unequivocally an historical turning point for intelligence and mass surveillance in modern societies. In response, many Western countries passed antiterror legislations that include language pertaining to police powers enhancement and, in the United States specifically, limitations of certain civil liberties such as privacy rights, right against self-incrimination, and protection from arbitrary searches. These changes have directly impacted how intelligence agencies operate. For instance, the US

National Security Agency (NSA) was permitted to routinely and systematically spy on its own citizens to uncover terrorist plots in the United States while the Central Intelligence Agency (CIA) was allowed to conduct torture and rendition programs in order to collect intelligence from so-called “enemy combatants.” The two long wars in Afghanistan and Iraq that followed the 9/11 attacks also impacted intelligence and surveillance activities by spurring the development of new intelligence practices such as predictive analysis of improvised explosive devices (bombing clusters) and the extensive use of drones for reconnaissance as well as bombings.

In 2007 and 2008, Russia launched two cyberattacks against Estonia and Georgia. These denials-of-services attacks were perpetrated against both government institutions such as parliament and ministries, as well as private organization like banks, newspapers, and broadcasters. These two attacks signaled a new type of warfare and the necessity to recognize the importance of the cyber world as a new battlefield where rogue states, violent nonstate actors, and organized crime can conduct activities that pose risks to modern and technology-dependent societies. Today, cyberspaces like the Internet and the Dark Web are heavily monitored and constantly targeted by national security and law enforcement intelligence operations alike.

In 2011, several countries in North Africa and the Middle East experienced civil unrest and civil war in the wake of the so-called “Arab Spring.” This global phenomenon was not foreseen by any intelligence communities in the Western world and emerged as a surprise to most international news outlets. Not only did foreign intelligence agencies fail to predict this social and political awakening, but most secret police systems in the countries affected by the unrest were totally blindsided by the technological prowess of the youth, who used social media avenues such as Facebook and Twitter in particular to circulate activist information and organize logistics for events. Before the events of the Arab Spring, the intelligence community never fully grasped the idea that political activists were capable of rapidly igniting a vast social movement, thereby challenging the status quo in several countries simultaneously.

In 2016, Russia was able to demonstrate its ability to harness its capability in the cyberspace to interfere in the presidential election. If this information warfare operation was not something new, its scope and intensity was certainly without precedent. Intelligence agencies from foreign countries were able to conduct vast disinformation campaigns on social media; hack, steal, and leak sensitive information from the Democratic National Committee; and sow discord to increase political polarization in favor of the Trump presidential campaign. This well-orchestrated cyber intelligence operation happened with little to no challenge from the US Intelligence Community. This event reminds us that a democracy can be hacked by virtual malicious actors through sophisticated intelligence operations and illustrate the necessity to develop a deep understanding of the intersection between technology, surveillance, and national security.

The interpretation of both existing knowledge and signals of new dangers have been challenging for law enforcement and national security intelligence agencies at many points during the past 30 years. The aforementioned critical political and social changes have demonstrated the limitations of states' knowledge about emerging global and national threats. Furthermore, the influence of international and national events on the security of modern society and the evolving mission of intelligence agencies have raised concerns among citizens about the lack of limitations on surveillance and the pitfalls of a state's control. The content of this book is geared toward anyone who seeks to understand the intelligence environment in modern times and is important reading for the general public, government and civilian employees, law enforcement leaders, military officers, private sector professionals, academics, and students. As a useful tool to support teaching at the graduate and professional education level, this book provides a broad understanding of current and emerging issues related to intelligence activities and offers a unique way of thinking about contemporary challenges in this field.

A comprehensive understanding of issues in the fields of intelligence and state surveillance is essential to the modern workforce and public that must function successfully in this current security climate. Members of the government, military, and private sector industry may find particularly interesting the reflection and research results related to the implementation of successful intelligence and surveillance strategies as well as frameworks for creating such strategies. This work also addresses the complexity of the world in which intelligence activities occur and, as such, is a useful tool for mid-level managers and high-level public sector administrators. It also explains both wanted and unwanted impacts of certain policies, laws, and regulatory frameworks on intelligence and surveillance activities.

This book assumes the readers have a basic understanding of intelligence operations, though it does not illustrate points through use of excessive jargon or overly elliptical theoretical discussion. However, it is not a purely descriptive manuscript, and does not aim to oversimplify matters at hand. The book, while not overly technical, still requires basic knowledge of intelligence collection, information analysis, international affairs, homeland security, protection of infrastructure, and related disciplines. It is my hope that the reader comes away with a more thorough understanding of how the dynamics between the security of the states and the risk society modulate intelligence and surveillance activities.

Frederic Lemieux
Georgetown University
Washington, D.C.
July 2018

Acknowledgment

This book represents a major contribution to the field of intelligence, and achieving this objective in a short period of time during a turbulent period of my life was a heavy demand. First of all, I would like to thank Jules Willan at Emerald Publishing Ltd for your trust in my work and for this productive professional relationship. The confidence she had in the project and her judicious advices were instrumental to the realization of the book. I am also deeply indebted to my special assistant, Melinda Hull, who worked hard on the revision and editing of the chapters. Thank you Melinda for having been flexible and reliable and for offering excellent suggestions throughout the editing process. Finally, I would like to thank the senior management at Georgetown University who gave me flexibility to complete this work while incepting and managing new graduate programs in intelligence and cybersecurity.

Nature and Structure of Intelligence: An Introduction

This book examines the evolution of state entities' surveillance in modern societies and provides an international perspective on several influential trends that have affected intelligence activities during the past 25 years. Since the dissolution of the Soviet Union in the early 1990s, state surveillance and intelligence activities in Western countries have transformed drastically, adapting to new domestic and global challenges. Law enforcement agencies have adopted and integrated new forms of crime management models, relying heavily on the use of intelligence and criminal analysis to tackle serious crime. Additionally, Western national security intelligence agencies redirected their interest from state actors, former Soviet Union, to new nontraditional threats such as international terrorist groups and low-intensity conflict or special warfare.

For a long time described as "two solitudes," due to their separate missions, mandates, and accountability structure, law enforcement and national security intelligence agencies are now engaged in intensive collaboration to address both international and domestic threats. This situation has blurred the lines between (1) interior and exterior security; (2) common crime and crime against the state; (3) civil liberties, privacy, and intrusive surveillance activities; and (4) strategic national security intelligence and operational military intelligence requirements. Nowadays, national and local law enforcement agencies conduct intelligence operations against international terrorist groups in their local and regional jurisdictions while national security intelligence organizations infiltrate organized crime operations and intercept a significant portion of their citizens' communications on a daily basis. Other important trends that are reshaping the state's surveillance and intelligence apparatus in modern societies include the use of cyberspace for information collection, the expansion of surveillance technology penetrating citizens' everyday lives, and the rise of the private sector as a primary surveillance facilitator or third-party actor in the collection and dissemination of national security intelligence.

This chapter is divided into six sections. The first section provides a succinct historical overview of the evolution of intelligence activity and strategy. The second section addresses the difference between domestic and foreign intelligence. The third section focuses on the intelligence process and its different components. The fourth section scrutinizes five intelligence domains and how they apply to

Intelligence and State Surveillance in Modern Societies, 1–17

doi:10.1108/978-1-78769-171-120181001

foreign and domestic intelligence activities. The fifth section examines several limitations related to the intrinsic nature of intelligence but also to the constraints posed by organizational bureaucracy specifically. Finally, the last section describes the structure of the book and introduces each chapter included in the book.

Historical Evolution of Intelligence

Since ancient times, intelligence activities were primarily used by emperors, kings, and warlords of the earliest societies to foresee the future and make strategic decisions to assert and solidify their power. For instance, in the Arab world, the role of the vizier was to provide advice to, and sometimes rule on behalf of, the Sultan or Pharaoh (Den Boorn, 2014). In ancient Greece, the oracles and prophets were consulted by kings who sought wise counsel before launching military campaigns or making important decisions for their people (Stoneham, 2011). Sub-Saharan African tribal chiefs also sought prophecies from various oracles (Webster & Boahen, 1968). In South America, the Mayas' powerful leaders consulted the chilanes or oracles to foresee the future of their reigns (McVeigh, 2017). In ancient China, kings consulted the oracle bones for advice on a variety of matters, including statecraft (Raphals, 2013). Though the foundation of their predictive capability was mostly inspired by divine or supernatural visions, viziers, oracles, and prophets in some societies did advise the ruler based in part on information they routinely gathered from spies and scouts. Spy networks and agencies were particularly renowned for their effectiveness in the Persian, Greek, Roman, Byzantium, Chinese, and Muscovy empires by being an essential part of the state bureaucratic structures and by systematically intercepting written messages communicated between cities (Dvornik, 1974). Espionage activities also netted information about foreign militaries and economic practices from traders, merchants, sailors, and other businessmen (Russel, 1999). Scouts were used to infiltrate unconquered territories and assess the strengths of other civilizations or tribes (Crowdy, 2011).

During the Middle Ages, religious institutions such as the Catholic Church developed a formidable network of spies during the Roman Inquisition (Thomsett, 2011). The Vatican relied on spies to identify heretics, political dissidents, and practitioners of witchcraft in France, Italy, and Spain. Through the Holy Office, which was charged with maintaining the political integrity of the Roman Catholic Church, cardinals and inquisitors operated a vast network of informants that were used in mass trials. In addition to using spy networks, the intelligence collection process also relied heavily on torture, achieving infamy for the Inquisition chambers (also known as test chambers) and their sheer brutality (Thomsett, 2011).

During the Renaissance era, the use of espionage became less a tool of the Church, as it became established within emerging states' structures and institutions. Espionage played a key role in the race for new world exploration, expansion, and protection of trade activities, and to support military campaigns (Mallett & Hale, 2006). It is during the Renaissance period that the use of spies was praised by Niccolò Machiavelli, the author of two major books related to state governance and the use of military force: *The Prince* and *The Art of War*. In his book *The Prince*, Machiavelli states that governing is to make people believe, thereby placing an emphasis on the role of influencing and deceiving masses instead of using force. In *The Art of War,* Machiavelli proposes 27 rules of war which offers this advice: "Counsel with many on the things you ought to do, and confer with few on what you do afterwards (p. 112)," alluding to the risk that rulers face of being spied on by the enemy's informants or double-crossed by their own. These two books, in addition to existing classics such as Sun Tzu's *Art of War,* clearly depict the importance of intelligence as a foundational component of governance.

During the period of 1700–1900, espionage and intelligence activities evolved rapidly and drastically. The emergence of new republics such as the United States and France generated a considerable need for domestic espionage dedicated to identify and track those who were loyal to the monarchy. Maximilien Robespierre and General George Washington both extensively utilized intelligence to undermine the monarchy regimes to which they were subject, through games of spy. For instance, George Washington used the Culper Ring to spy on the British headquarters based in New York, providing valuable intelligence on British troops' movements (Daigler, 2015). In France, the "terror regime" of Robespierre institutionalized the role of informants by creating a formal reward system through the Revolutionary Law (Zimmermann, 2013). In 1799, Napoleon Bonaparte ousted Robespierre's Revolutionary Regime through a military coup and proclaimed himself Emperor of France in 1804. Immediately following his elevation to power, Napoleon launched several efficacious war campaigns in Europe and placed an emphasis on the use of spies on the battlefield. As Napoleon stated: "One spy in the right place is worth 20,000 men in the field" (Lathrop, 2008: 135).

The industrial revolution in the nineteenth century brought a new form of intelligence with it: industrial espionage. Governments in several European countries used informants to spy on workers' unions and protesters. The industrialization revolution was rife with clashes between political dissidents (radical workers) and the government, thereby creating an urgent need for domestic intelligence in order to better control social movements (Hopkins, 2013). Labor organizations were also regularly using spies to gather information to publicly denounce working conditions in many factories. This era is also associated with the emergence of new technologies designed for the concealment, transcription, and analysis of intelligence (Janeczko, 2012). For instance, photography, telegraph and Morse code, invisible ink, and new forensic methodologies played transformational roles in the evolution of intelligence activities.

The twentieth century brought dramatic transformations in the intelligence activities and surveillance capabilities of governments. For instance, World War I provided an opportunity for the British, French, and American militaries to cooperate not only in the exchange of intelligence but also in combat experience and practices (Gilbert, 2012). It is also during the period encompassing World War I that the United States established its communication intelligence agency in the Army, the predecessor of the National Security Agency (NSA). During World War II, the intelligence activity of several nations including Great Britain, Germany, Japan, and the United States were focused on communication interception, code breaking, and encryption of messages through complex machines such as the German Enigma cipher machine.

The Cold War was one of the most intense spying periods of modern history. Espionage between Western countries and the Soviet Union was mainly conducted by paying informants, using double agents, stealing documents, intercepting communications, and via listening and viewing devices. This period was characterized by the development of a plethora of spying gadgets, including perhaps the most sophisticated one of that time: the surveillance satellite. In the early 1960s, the United States launched its first reconnaissance satellite programs named Corona and Zenit. Only capable of providing photography surveillance of preselected areas on the earth in the early stage, reconnaissance satellite programs evolved rapidly, offering a broader range of capabilities including early missile warning, nuclear explosion detection, electronic reconnaissance, and radar imaging.

The end of the Cold War era was characterized by the diffusion of disruptive innovations such as cellular communications, computers, and the Internet. These significant innovations directly contributed to the globalization of communication and facilitated global mass surveillance through programs such as Echelon, a surveillance program operated by five cooperating countries. The twentieth century was also a critical period for the growth of intelligence agencies in modern societies due to the nature of their missions (domestic or foreign) or their areas of specialization (intelligence domains).

Dual Conceptualizations of Intelligence

The ratification of the Westphalia treaties in the seventeenth century aimed at restoring peace in Europe, but also created the foundation for self-determined rules as well as what came to be known as the Westphalian sovereignty. In this context, the principle of sovereignty pertains to the idea that inter-nation interference in domestic affairs and direct aggression must be held in check by a balance of power between states and respect for a state's territorial integrity (Kegley & Wittkopf, 2005). In order to protect themselves against other nations' intrusions, many countries made a distinction between foreign and domestic threats, subsequently impacting policy, strategy, and practices. For instance, Napoleon Bonaparte used a network of spies and scouts in his war campaigns through Europe to acquire more intelligence about the military capacities and political intentions of other European countries (foreign threats). During Napoleon's reign, the Minister of Police, Joseph Fouché, was tasked with keeping peace at home. In order to ensure that no foreign nation would interfere and destabilize France's domestic affairs, Fouché operated a vast network of informants spanning across the country in order to prevent or counter any agitation within the population (domestic intelligence operations). According to L'Heuillet (2001), Fouché perceived the citizenry as potential political force that could destabilize the empire and impose its own law. Therefore, the role of police is political in the sense that it should monitor the population in search of dissention. A notorious myth surrounding Fouché was spreading the myth that no group of three persons or more could assemble and criticize public affairs without him being informed (L'Heuillet, 2001). In actuality, no such law existed. L'Heuillet explains the French police concept and practice in terms of a "panoptic binocular" due to the police's ability to observe its own populace. This is reminiscent of Jeremy Bentham's (2009) "panopticon" concept where all inhabitants of a particular area are able to be observed from one point without knowing they are being observed.

According to Brodeur (2010), policing activities conducted by the state can be characterized in two manners: high and low policing. High policing refers to the activities in which the state is engaged in protecting itself against physical or ideological attacks. A high policing model is characterized by specific elements, such as "protection of the political regime; the state defined as victim; the retention of information until it can be used with maximum efficiency; the utilization of known criminals; the use of informants; secrecy; deceit; the conflation of executive, judicial, and legislative powers; and extra legality" (Brodeur, 2010: 223). On the other hand, low policing refers to a more democratic model in which police address more common crimes and public disorders. High policing activity happens in an atmosphere of political opaqueness where the *raison d'état,* or reason of State, is often claimed over civil liberties and due process.

However, low policing activities are subject to more scrutiny by citizenry through public complaint processes, courtroom procedures, and constitutional protections and are more directed toward the protection of goods and people (e.g., Bill of Rights). Low policing can also be characterized by overt or covert activities (Brodeur, 2010). Overt low policing refers to visible daily policing, which pertains to property crime, disputes between citizens, and traffic regulations. Covert low policing refers to invisible police activity conducted through the use of informants, electronic surveillance, and undercover operations. Covert low policing techniques are comparable to those used in high policing activities and they are based on similar premises: deception and secrecy.

Another example of a dual conceptualization of intelligence is the distinction between national security intelligence and criminal intelligence. National security intelligence refers to information gathered and analyzed to protect the physical integrity of a country (military defense) as well as against any threats to the economy, energy infrastructure, environment, political system, or any other sectors that could be critical to the stability of a given state (Johnson, 2016). Agencies involved in the performance of national security intelligence activities are diverse and involve both foreign and domestic security apparatuses. The concept of criminal intelligence activities refers to information gathered and analyzed to support operational and strategic law enforcement missions (Ratcliffe, 2016). Criminal intelligence activities are generally used to better understand existing and emerging threats in the criminal environment. Over the past several decades, criminal intelligence activities have focused on organized crime and particular forms of crime such as serial killing, crime concentration, fraud, etc.). Most criminal intelligence activities are conducted at the domestic level through local and national law enforcement agencies. However, some supranational agencies such as Interpol and Europol facilitate the exchange and the analysis of criminal intelligence concerning transnational crimes.

Since the tragic events of September 11, 2001, the dual conceptualization of intelligence has been profoundly transformed in many Western countries. For example, in the wake of 9/11, many allies of the United States passed comprehensive legal reforms related to national security and counterterrorism issues. In most cases, these legal reforms blurred the line between domestic and foreign intelligence collection and analysis as well as blended the national security and criminal intelligence missions. Table 1 illustrates the traditional interrelation between the types of intelligence missions (national security and criminal) and the origins of security issues (foreign and domestic). Although, it is critical to understand that since September 11, 2001 the line separating or distinguishing between national security and criminal intelligence has become more porous. Consider the case of terrorism and the various approaches to counterterrorism in practice around the world. In countries that have adopted a judiciary model of counterterrorism, political violence is defined as a crime, terrorists are criminals, and law enforcement is the preferred institution to tackle this national security issue. However, in countries that have adopted a warfare model of counterterrorism, political violence is defined as an act of war, terrorists are enemy combatants, and the military is the chosen institutional tool to tackle this national security issue. In the case of the judiciary model, the police use a covert low policing approach to terrorism activity and the objective is to gather intelligence and ultimately produce evidence to obtain a conviction in criminal court. In the case of warfare model, the military institution uses intelligence to identify and neutralize the enemy combatants through capture or physical elimination. In the warfare model, the state often suspends the rights and civil liberties of its own citizens, as in the case of Anwar al-Awlaki, a US citizen killed in Yemen in 2011 by a US drone.

Table 1: Comparison Between the Types of Intelligence Activities and the Nature of Security Threats.

	National Security	**Criminal**
Domestic	Counterterrorism and Counterintelligence activities	Criminal analysis and intensive police tactics against serious crimes
Foreign	Spying of/on foreign states as well as nonstate actors and support military activities	Support international criminal investigations and exchange criminal intelligence between states through supranational structures

Moreover, it is important to mention there are agencies oriented toward foreign national security intelligence collection spying on their own citizens (domestic activities) or monitoring the activities of international organized crime (criminal intelligence). Local law enforcement (criminal intelligence) also conducts foreign national security intelligence collection designed to protect large urban areas against terrorist attacks through deployment of international police attachés (foreign threats). There is also an increase of local law enforcement conducting domestic national security intelligence collection through sting operations in order to identify and foil potential lone-wolf terrorist attacks inspired by foreign propaganda.

Intelligence Collection Disciplines

According to Lowenthal and Clark (2015), intelligence activity is characterized by five major collection disciplines. Historically, intelligence activity was mainly oriented toward two primary domains: human intelligence (HUMINT) and open-source intelligence (OSINT). HUMINT refers to the exploitation of human sources such as spies or undercover agents that provide critical data related to targets of interest. OSINT refers to data publicly available through digital or hard copy open sources such as news media, government reports, databases, books, journals, and the Internet. During the twentieth century, new technologies have significantly enhanced intelligence capabilities by creating additional domains: measurement and signature intelligence (MASINT), imagery intelligence (IMINT), geospatial intelligence (GEOINT), and signals intelligence (SIGINT). MASINT refers to the utilization of data related to the measure of electro-optical, nuclear, geophysical, radar, radiofrequency, and material sources. IMINT refers to pictures and images that analysts interpret to give a meaning to the content. GEOINT refers to the use of imagery (IMINT) and geospatial information related to a target of interest such as a physical feature (building or natural features) and human activities around it. Finally, SIGINT refers to the interception and usage of telecommunication, electronic communications, and telemetry activity. The data collected from these different disciplines can be qualified as structured or unstructured. Structured data are data that are contained in fixed fields of records or files such as information contained in relational database or spreadsheets (MASINT and GEOINT). Unstructured data typically refer to descriptive, literal, and text heavy data that can include some structured data such as date, phone numbers, bank accounts (SIGINT, HUMINT, OSINT). Table 2 presents the application of the six intelligence collection disciplines or domains according to the intelligence fields (national security and criminal).

The Intelligence Process

According to Fingar (2011: 4), the mission of intelligence is to "evaluate, integrate, and interpret information in order to provide warning, reduce uncertainty, and identify opportunities." The intelligence process allows analysts to connect knowledge about trends, security problems, international perception, and political

Table 2: Intelligence Collection Disciplines and Their Application to Intelligence Fields.

Disciplines	National Security	Criminal
HUMINT	Mole, spy, prisoner	Informant, undercover agent, victim, suspect, witness
SIGINT	Interception of all forms of electronic communication (cell phone, email, radio, social media)	Interception of phone communication (wiretap) and surveillance of social media
GEOINT	Satellite imagery, drone surveillance	Drone surveillance, crime mapping
MASINT	Missile tracking, nuclear radiation detection, weather and sea data, electromagnetic pulse	Cybersecurity, forensic analysis, gunshot detection
IMINT	Photography from imagery satellites, drones, physical surveillance, cell phones, social media, and CCTV	Photography and imagery from drones, physical surveillance, cell phones, social media, and CCTV
OSINT	Media, public data, professional and academic literature, web-based communities, wikis, blogs	Media, public data, professional and academic literature, online satellite photography, geographic information systems, wikis, blogs

calculus of foreign nations to policy and decision-making processes. Intelligence analysts have the responsibility to provide objective, accurate, and timely intelligence products to support a variety of stakeholders. Intelligence is usually defined as the end result of a process cycle composed of several steps, which includes (1) priorities and intelligence requirements (PIRs); (2) data collection; (3) data collation; (4) data analysis; and (5) intelligence dissemination. Another important step of the intelligence cycle is the (6) evaluation of intelligence (Peterson, 2005). While most authors identify the evaluation of intelligence as the last step of the cycle, the work of Lemieux (2006) shows that assessment procedures are in fact happening all along the intelligence process. Therefore, Fig. 1 illustrates this reality by placing the evaluation step at the core center of the cycle as a reminder of its importance as it relates to the integrity of the intelligence product. The intelligence cycle recognized by several professional communities is very similar to the research methodology process used in academia, with the exception that the intelligence process aims to produce actionable knowledge