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

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

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

First edition 2019

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

Certificate Number 1985
ISO 14001

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

This page intentionally left blank

List of Tables

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.