# Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

– biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
– crisis and disaster management
– terrorism
– cyber security and secure information systems (e.g., encryption, optical and photonic systems)
– traditional and non-traditional security
– energy, food and resource security
– economic security and securitization (including associated infrastructures)
– transnational crime
– human security and health security
– social, political and psychological aspects of security
– recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
– smart surveillance systems
– applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Bryanna Fox • Joan A. Reid • Anthony J. Masys
Editors

# Science Informed Policing

Springer

*Editors*
Bryanna Fox
Department of Criminology
University of South Florida
Tampa, FL, USA

Joan A. Reid
Department of Criminology
University of South Florida-St. Petersburg
St. Petersburg, FL, USA

Anthony J. Masys
College of Public Health
University of South Florida
Tampa, FL, USA

# Introduction

The current policing landscape has seen the rise in serious and organized crime across the globe. Criminals are innovating in real-time, leveraging cyber, social media, enhanced surveillance to support their activities. In so doing, the criminal landscape has become transnational, whereby collaborative networks have flourished, creating greater complexity and novel threats for the international policing community. For example, with the onset of cybercrime as an evolving form of transnational crime, our previous understanding of forensics and criminal business models is challenged by the opaque nature of this criminal domain.

As new threats to local, regional, national, and global security are emerging, leveraging science and technology innovations has become more important. Advances in big data analytics, cyber forensics, surveillance, modeling, and simulation have led to a more data-driven, hypothesis-generated, and model-informed approach to policing, crime prevention, and understanding and deterring offenders. Novel science and technology innovations are presented here to provide insights and pathways that challenge the emerging and complex criminal threat landscape by supporting policing operations.

This edited book explores science and technology innovation and its applications to the policing community. It is divided into two parts:

1. Policing and Crime Prevention
2. Policing Tools and Strategies

## Policing and Crime Prevention

Jaynes and Loughran in their chapter "How Offender Decision-Making Can Inform Policing: A Focus on the Perceived Certainty of Apprehension" argue that the perceived certainty of apprehension is a far more effective deterrent than the severity of sanctioning. In concordance with this, many policing strategies have focused on increasing the certainty of apprehension as a key tactic in crime reduction. This

chapter describes how recent advances in criminological understanding of perceived certainty are thought to influence offender decision-making. They then illustrate how these findings may inform policing and suggest potential avenues for collaborations between researchers and practitioners to further enhance understanding of offender decision-making and guide evidence-based policing.

Finnegan and Masys in their chapter "An Epidemiological Framework for Investigating Organized Crime and Terrorist Networks" argue that epidemiology, the science of public health, provides a unique approach that can be leveraged and tailored to support policing operations. The systems lens is key to the application of epidemiological models, and hence, the Cynefin framework is introduced to help frame the policing problem space in terms of complexity. This chapter presents a conceptual model that illustrates and operationalizes epidemiological practices to support policing operations.

Chopin and Beauregard in their chapter "Sex Offenders' Forensic Awareness Strategies to Avoid Police Detection" argue that one of the most important costs for offenders is to be identified and arrested by police. In order to avoid arrest, offenders have to rely on specific strategies for "success". In sexual assaults, in addition to appropriate target selection, offenders must make sure to avoid police detection by protecting their identity and cleaning up or destroying forensic evidence that may be left at the crime scene and that can directly lead to their identification. This behavior is known as "forensic awareness." Research on forensic awareness strategies during the crime-commission process is scant. A number of studies looking specifically at sexual crimes identified certain strategies related to forensic awareness. According to the rational choice perspective, the use of strategies to avoid police detection should have an impact on the crime solving by police. Few studies have investigated this issue, and findings are quite unexpected. The aim of this chapter is to review some of the most important empirical knowledge on the use of forensic awareness strategies in sexual crimes.

Shortland and Forest in their chapter "Tracking Terrorism: The Role of Technology in Risk Assessment and Monitoring of Terrorist Offenders" present how technology is increasingly used to help expand the amount of information collected about potential terrorist threats. However, it is clear that an equally important (if not more important) part of these efforts is the ability to separate, within the mass of individuals (or data) identified, those individuals who will conduct acts of terrorism (the minority) from those who will not (the majority). Thus, a core challenge is how information is handled, interpreted, analyzed, and used to inform decisions. In this chapter, they discuss the dynamic interplay between the collection of intelligence (including technology-assisted surveillance) and decision-making. Specifically, they focus on how issues in our understanding of "the terrorist" interact with and impact the use of technology within counter-terrorism. In addition to this, and in support of future research in this area, they highlight some innovative areas for growth and new avenues to facilitate the integration of technology within counter-terrorism.

Reid and Fox in their chapter "Human Trafficking and the Darknet" describe how in an era of unprecedented technological accessibility, coupled with the possi-

bility of online anonymity, human traffickers often operate in the shadows – avoiding interference by typical societal safeguards and law enforcement. This chapter highlights challenges to combatting human trafficking due to the widespread use of mobile technology and the anonymity of the Darknet. The chapter reviews criminal justice resources devoted to combatting human trafficking facilitated by the Internet.

## Policing Tools and Strategies

Borum in his chapter "Scientific and Technological Advances in Law Enforcement Intelligence Analysis" describes how a range of professions and business enterprises have moved toward a more science-driven approach to operations. Law enforcement has been no exception. In fact, the modern-day idea of intelligence-led policing (ILP) emerged in the UK in the 1990s as the country was pushing all government services to operate on more of a data-informed, business process or managerial model. This trend led to the development of a British "National Intelligence Model" (NIM), which by 2002, was formally adopted as policy for law enforcement agencies nationwide. ILP has surged in popularity among US law enforcement agencies, although what exactly ILP means in an operational sense and how it is implemented vary considerably. This chapter will not focus primarily on the programmatic aspects of ILP but on scientific and technological advances that have enhanced and accelerated the intelligence analysis process for policing applications.

Houck in his chapter "Improving Criminal Investigations with Structured Analytic Techniques" discusses how the intelligence community has used structured analytic techniques, which are methods designed to reduce bias and increase transparency of process, for years. The techniques force analysts out of routine thinking and away from heuristic habits in order to increase creativity, more comprehensively evaluate the questions, and create a document trail that reveals the thinking process that led to the intelligence product. These methods can be adapted for use in criminal investigations to help reduce bias, improve accuracy, and avoid both wrongful convictions (over 2200 to date) and reparations (more than $2.2 billion) while optimizing resources. The methods shift the investigator from intuitive, daily thinking (System 1 in Kahneman's terminology) to a more analytical approach (System 2) that creates a transparent process, regardless of the outcome. Structured analytical techniques are simple to use, inexpensive, and largely visual; they promote transparency, creativity, and group discussion, leading to better-supported results.

Houck in his chapter "Front-End Forensics: An Integrated Forensic Intelligence Model" describes how forensic science has the ability and capacity to be an active participant in investigations, rather than its traditional passive role. Too often, the evidence is collected and submitted to the laboratory, and the investigators wait for results, creating a lag between when the information is needed and when it is made available. Obstacles to forensic service providers being actively involved in investigations include organizational cultural norms, operational resources, sworn and

civilian human resource issues, and media-driven expectations of outcomes. While traditional intelligence analysis is forecasting, forensic science and criminal investigations are reconstructive, and this alters which methods can be and how to improve investigations. What has been characterized as forensic intelligence in the literature is largely forensic support to crime analysis. The benefits to using actual forensic intelligence actively in investigations by shifting forensic results, even if preliminary, to the front-end of the criminal justice system are reduced wrongful arrests and convictions, more efficient use of policing resources, and stronger cases for adjudication. An integrated forensic intelligence model (IFIM) is offered as a roadmap to creating a sustained professional culture of forensic intelligence.

Jeanis in her chapter "Missing Persons and Runaway Youth: The Role of Social Media as an Alert System and Crime Control Tool" argues that missing persons cases have a unique relationship with the media, where increased exposure is said to be a key factor in the recovery of victims and closure of cases. In an attempt to increase exposure for certain types of missing persons cases, news media outlets share case content and alert systems were created; however, the current systems in place have notable limitations. In an attempt to adapt to the proliferation of social media in the lives of everyday Americans, law enforcement agencies have begun to rely on social media as a crime control tool and as a means to raise awareness of missing persons cases. This chapter serves as an overview of the current academic standing of social media as a mechanism of crime control, with a specific focus on how law enforcement can optimize their use of social media in the form of a missing persons outreach tool.

Farrell, Wills, and Nicolas in their chapter "Police Engagement in Multidisciplinary Team Approaches to Commercial Sexual Exploitation of Children" describe how over the past two decades law enforcement has been given new mandates to identify and respond to the commercial sexual exploitation of children (CSEC). While CSEC has been identified as an important community safety issue and the negative impacts on young people are well documented, it has proven to be difficult for the police to identify young people who are at risk of victimization and challenging to develop the trust necessary to gather information needed to support investigations, arrest perpetrators, and provide safety to child victims. In response to these challenges, law enforcement is increasingly partnering with child welfare and service provider stakeholders to improve responses to CSEC in local communities. This chapter describes the problem of CSEC and outlines key aspects of a multidisciplinary team approach to the problem. Using qualitative interview data from participants in six multidisciplinary teams in Massachusetts dedicated to responding to CSEC, they discuss key benefits and challenges to a multidisciplinary team approach to CSEC.

Bennett in his chapter "The Lived Reality of Police Helicopter Operations: Frank and Revealing Interviews with National Police Air Service Personnel" reveals the lived reality of police helicopter operations in England and Wales, from witnessing acts of extreme violence (such as a beheading in North London) to searching for the remains of bodies atomized by locomotive impacts. Highly professional in their outlook and behavior, the men and women of the National Police Air Service

(NPAS) push themselves and their equipment to the limit in their quest to safeguard the public and apprehend criminals. Interviewees claimed a link between teamwork training and performance. Teamwork training – known in aviation as crew resource management – was universally praised. It is recommended that the police service urgently considers the introduction of teamwork training for all officers. The police service is starved of resources. The NPAS needs better equipment – longer-ranged, more capable helicopters with state-of-the-art sensors and communications equipment and protection from small arms fire. The State's primary mission is to ensure the safety and security of its citizens. As a matter of urgency, the government should divert monies from healthcare and education to the police service. Integrity and courage should be recognized and rewarded.

Masys in his chapter "Science Informed Major Event Security Planning: From Vulnerability Analysis to Security Design" describes how the post 9/11 security landscape has seen a fundamental shift in security planning, organization, and management across the national and global security domain. This shift is particularly evident with regard to special events. Major national regional and global events such as the Olympic Games, FIFA World Cup, the US Super Bowl, and the Boston Marathon draw large crowds of spectators and participants, thereby creating vulnerable targets. The 1972 Munich Olympics and 1996 Atlanta Olympics are two examples of pre-9/11 attacks on sporting events. Since 9/11, we have seen attacks on events such as the Boston Marathon in 2013, Las Vegas active shooter in 2017, and the bombing in Manchester at the Ariana Grande concert in 2017. These examples highlight the inherent vulnerabilities and security challenges that reside in major events (sporting, cultural, religious, musical). With this in mind, security budgets have increased to deal with such risks and threats. For example, the security budget for the 2012 London Olympics topped $1.46 billion and the 2010 Vancouver Olympics was over $900 million.

This chapter examines the security challenges and solutions for managing major event security. Scenario planning and disaster forensic methodologies are presented along with the role of predictive analytics in supporting vulnerability analysis and security solution navigation. Key recommendations are made pertaining to vulnerability analysis and the development and design of a security architecture planning framework rooted in a high reliability security organizations.

# Contents