Scientific and Technological Advances in Law Enforcement Intelligence Analysis

Randy Borum

Abstract Powered by advances in computing technology, 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. "The NIM followed the government policy of using a business process model to deal with crime control and employed the ILP philosophy to introduce intelligence into virtually all aspects of the policing business plan" (p. 311).

ILP has surged in popularity among US law enforcement agencies, although what exactly ILP means in an operational sense, and how it is implemented varies considerably (Ratcliffe J, Intelligence-led policing. Routledge, New York, 2016). At the most basic level, ILP is commonly defined as "the collection and analysis of information related to crime and conditions that contribute to crime, resulting in actionable intelligence products intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats" (Carter DL, Carter JG, Crim Justice Policy Rev 20(3):310, 2009, p. 317). Although sometimes broadly considered, ILP has become widely used. It is not a "program," but more of a philosophy and approach for meeting a law enforcement agency's mission objectives. 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.

Keywords Intelligence led policing · National intelligence model · Law enforcement · Data

R. Borum (✉)
School of Information, University of South Florida, Tampa, FL, USA
e-mail: borum@usf.edu

B. Fox et al. (eds.), *Science Informed Policing*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-41287-6_6

1 Introduction

Powered by advances in computing technology, a range of professions and business enterprises have moved to 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. "The NIM followed the government policy of using a business process model to deal with crime control and employed the ILP philosophy to introduce intelligence into virtually all aspects of the policing business plan" (p. 311).

ILP has surged in popularity among US law enforcement agencies, although what exactly ILP means in an operational sense, and how it is implemented varies considerably (Ratcliffe 2016). At the most basic level, ILP is commonly defined as "the collection and analysis of information related to crime and conditions that contribute to crime, resulting in an actionable intelligence products intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats" (Carter and Carter 2009, p. 317). Although sometimes broadly considered, ILP has become widely used. It is not a "program," but more of a philosophy and approach for meeting a law enforcement agency's mission objectives.

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. We begin by defining intelligence and differentiating it from crime "data" or crime-related information, then we briefly discuss progress in the professionalization of law enforcement intelligence as a field of practice. Next, we demonstrate how science has helped advance the "human" dimensions of analytic tradecraft. Finally, we review recent developments in computing and in information and communication technology that have enabled analytic advances for policing applications.

1.1 Intelligence, Data and Information

Too often, the term "intelligence" is used casually, even in law enforcement parlance, to refer to crime data, statistics, or any potentially useful points of crime-related information. Intelligence may build on data or information, but the terms and concepts are not synonymous. In the field of Information Science there is a widely acknowledged hierarchy of information-related content, centered on four concepts: data, information, knowledge and wisdom (DIKW) (Ackoff 1989). Sometimes "understanding" is considered a separate category between knowledge

and wisdom. Each cumulatively builds upon the other. In fact, this particular stack is often called the DIKW Hierarchy or just the "Information Hierarchy" (Rowley 2007). Systems theorist, Russell Ackoff (1989), defined the elements of this construct in the following way:

- Data: symbols with no inherent meaning
- Information: data that have been given meaning; provides answers to "who", "what", "where", and "when" questions
- Knowledge: application of data and information; answers "how" questions
- Understanding: appreciation of "why"
- Wisdom: evaluated understanding.

In this hierarchy, information is defined in terms of data, knowledge is defined in terms of information, and wisdom is defined in terms of knowledge (Rowley 2007). Analysis is the mechanism to get from data to information and from information to knowledge, understanding, and wisdom.

Intelligence, akin to "wisdom" in the Information Hierarchy, is a high-level concept. It is not just "processed" information; rather intelligence refers to the actionable insights derived from analyzed and evaluated information. As intelligence expert Robert Clark (2019) suggests: "A typical goal of intelligence is to establish facts and then to develop precise, reliable, and valid inferences (hypotheses, estimations, conclusions, or predictions) for use in strategic decision-making or operational planning" (p. 22). In that sense, intelligence is information in action, or in Michael Warner's (2002) words, "It is what people do with data and information that gives them the special quality we casually call intelligence" (p. 17).

Concerning Law Enforcement Intelligence, specifically, Carter (2009) offers the following insightful definition:

> intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem solving (that is, analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists (p. 9).

Data, information and intelligence have all supported law enforcement operations, but the strategic and tactical uses of intelligence have created a modern ethos of "evidence based policing." The status of intelligence in American law enforcement was markedly elevated in the wake of the 9/11 terrorist attacks. Those attacks were widely cited as resulting from a "failure of intelligence." In the post-9/11 era, federal, state, local and tribal law enforcement agencies were pushed to move from traditional approaches of response driven policing to more proactive approaches emphasizing prevention and risk management. They were also given a much more central role (and responsibility) for homeland defense and security. Improvements and advancements in law enforcement intelligence were often the centerpiece of those efforts.

Because intelligence is defined by the meaning educed from processed and analyzed information, all intelligence, including law enforcement intelligence, emerges from a recursive sets of tasks and activities, known as the Intelligence Cycle. The traditional intelligence cycle comprises the following five stages:

- **Planning and Direction**: The first stage involves establishing what intelligence the consumer/requestor needs to best inform her/his decision. The planner should identify not only she/he thinks the customer "needs to know," but what the consumer will *do* with the information. The intelligence points needed for the decision are known as "Intelligence Requirements." The requirements guide the plan for what data or information will be collected (as well as how and from where it will be collected), what kind of analysis or processing is needed, and to whom (and how) the finished intelligence product it will be disseminated.
- **Collection**: In the second stage, the raw data or information is collected in accordance with the plan. That data may come from publicly available information (Open Source) and/or from secret or classified sources, and may be gathered from straightforward searches of textual materials, queries of human assets, or through technical means (e.g., electronic, satellite imagery, measurements, etc).
- **Processing**: In the third stage, the raw data or information is processed into a usable form. That may involve decryption, language translations, technical measurement or statistical analysis. In the era of Big Data and information overload, a critical preliminary task for the processing stage may be data reduction – sifting through the "noisy" data and drilling down to the most vital and reliable points. This might be regarded as a type of "pre-processing."
- **Analysis and Production**: The fourth stage is where data becomes intelligence. An analyst evaluates and integrates all relevant data/information from various sources, attempts to "make sense" of it, and to draw inferences and conclusions with regard to the original intelligence requirements.
- **Dissemination**: In the fifth and final stage, the analytic assessment, a finished product, is provided to the intelligence consumer/requestor in a form that directly addresses the specified intelligence requirements. That will lead the intelligence consumer/requestor to determine whether the intelligence provided is sufficient, or whether additional intelligence requirements need to be prosecuted, which is the function of the first stage; hence, the cyclical nature of the process.

1.2 Human-Centered Advances in Intelligence

After 2001, as law enforcement agencies began building or growing their intelligence capabilities, demand grew quickly for qualified law enforcement intelligence analysts. Two related trends are especially noteworthy: (1) professionalization of law enforcement intelligence as a discipline and (2) the application of scientific knowledge to improve human analytic performance.

1.2.1 Professionalization of Law Enforcement Intelligence Analysis

Although intelligence and crime analysts have worked in law enforcement for decades, as a discipline, law enforcement intelligence analysis is still fairly young (Gentry 2016; Marrin 2016; Marrin and Clemente 2006). It was not until the 1980s that crime and intelligence analysts began networking, organizing and developing a collective sense of professional identity. The first professional association for law enforcement analysts— the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA)—only began in October, 1981. They currently have over 2500 members from more than 40 countries. A second organization emerged in 1990—the International Association of Crime Analysts (IACA). They currently claim over 4000 active members from more than 60 countries.

Both groups have worked toward developing standards of practice and "professionalizing" the discipline. Mature professions typically share certain characteristics, such as having recognized governing bodies, formal training and continuing education programs, certifications, a common body of knowledge and standard methods for knowledge discovery (research) and management. The field of intelligence analysis generally has made substantial progress in these areas over the past 40 years (Gentry 2016; Marrin and Clemente 2006). Law enforcement intelligence specifically is not quite as advanced, but is certainly moving forward.

Professional certifications and the standards that govern and drive them have been essential elements in the professionalization of law enforcement intelligence (Harrison et al. 2018). Both IALEIA and IACA have created professional certification programs for analytic professionals. IALEIA's program began in 1991. The certification was crafted initially through a partnership with the Society of Certified Criminal Analysts, but IALEIA has essentially subsumed that Society within its certification process. They currently have a four tiered system, beginning with a Basic Analyst Certification, and progressing to the Criminal Intelligence Certified Analyst (CICA). The CICA designation should reflect that the analyst "has demonstrated professional achievement in the intelligence analysis field though establishing an experience base, participating in ongoing training and development activities, and demonstrating analytic competency." Criteria include professional analytic experience, specialized analytic training and formal education concerning 17 content/skill areas.

After 9/11, The International Association of Chiefs of Police (IACP) and the Community Oriented Policing Services (COPS) convened the "Summit on Criminal Information Sharing: Overcoming Barriers to Enhance Domestic Security." A central conclusion from that Summit was that standards were needed for intelligence training. This call for professional standards was echoed in *The IACP Criminal Intelligence Sharing Report: A National Plan for Intelligence-Led Policing at the Local, State and Federal Level*, and the Summit recommendations were formally adopted by The Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG) Training Committee. The GIWG then set about reviewing and establishing best practices in law enforcement intelligence from federal, state, and local-level programs.

In October 2003, the Global Justice Information Sharing Initiative released a *National Criminal Intelligence Sharing Plan* (NCISP), and in 2005 the GIGWG, in cooperation with IALEIA, released a set of 25 *Law Enforcement Analytic Standards* for intelligence analyst certification programs and processes. The standards pertained to analyst education/training, professional conduct, and certification as well as standards for the analytic processes and products themselves. Concerning professional certification, the *Standards* made the following specific recommendation:

> *Analysts should be certified by an agency or organization (governmental, professional association, or institution of higher learning) program specifically developed for intelligence analysts. These analytic certification programs shall reflect experience, education, training, and proficiency testing* (Global Justice Information Sharing Initiative 2007, p. 1).

This call accelerated the field's movement toward widespread endorsement of analyst certification (Global Justice Information Sharing Initiative 2003).

IALEIA's certification was aligned with NCISP guidelines. Building on the NCISP mandate, IACA's professional certification program—the Certified Law Enforcement Analyst (CLEA)—began testing analysts in 2005. Criteria for the CLEA credential also include professional analytic experience, specialized analytic training and formal education to include 19 content/skill areas. Both the CICA and CLEA certifications have authoritative reference documents comprising a common body of knowledge for law enforcement analytic practitioners.

A comparison of the Certification domains for the CICA and CLEA certifications in provided in Table 1.

The experience, training/education and professional knowledge requirements for the CICA and CLEA credentials are substantially similar. IALEIA tends to focus more on strategic-level analysis (e.g., longer term, future-oriented assessments), while IACA tends to emphasize the tactical-level (e.g., immediate and short-term characterizations of the operating environment). Similarly, IALEIA tends to highlight more traditional, qualitative, expert-driven assessment methods (with roots in structured analytic techniques), while IACA has a more explicit focus on quantitative, data-driven methods (with roots in crime statistics and analytics). Law enforcement analysts in both organizations (and with both certifications), however, can

Table 1 Comparison of IALEIA and IACA knowledge domains

IALEIA's CICA exam domains	IACA's CLEA exam domains
Analytic techniques and methods	Crime analysis – terms, concepts and processes
Creative and critical thinking	Law enforcement models
Crime indicators	Criminal behavior
Crime pattern analysis	LE data and crime analysis data sources
Inference development	Internet resources
Information management – classifications, collation	Crime analysis data and data management
Information sharing	Applied research methods
Information sources	Descriptive statistics
Intelligence cycle/process	Advanced statistical concepts
Intelligence-led policing	Qualitative analysis
Intelligence product development	Spreadsheet operations
Legal, privacy, ethics issues	Temporal analysis
Logic	Intelligence analysis and intelligence charting
Recommendation development	GIS and crime mapping
Structured analytic techniques	Spatial analysis and forecasting
Strategic analysis	Effective analytical writing
Tactical analysis	Analytical products
	Applied crime series analysis
	Organized crime

operate across the strategic-tactical spectrum and may use qualitative and/or quantitative analytic methods; the difference is mainly a matter of emphasis. Both organizations and both professional certifications have helped to standardize and raise the bar for analyst qualifications, just as the *Law Enforcement Analytic Standards* and *Law Enforcement Analyst Certification Standards* have elevated law enforcement analytic practices, processes and products (Bruce and George 2015).

1.2.2 Applying Science to Improve Human Analytic Performance

Intelligence analysis relies on complex cognitive processes, to include evaluating and weighing evidence to test hypotheses and educe conclusions under conditions of uncertainty. There are well-known limitations to those cognitive capabilities, however, that can directly affect analytic outcomes. Two applications of science (i.e. the science of human judgment and decision making) have had a particular impact on human analytic performance in intelligence-related analytic tasks. The first occurred over several years as a senior CIA analyst sought to educate analysts on decision-making research, and look for ways to mitigate the impact of cognitive biases. The second was a large-scale program of research aimed at understanding how people make forecasts and predictions about geopolitical events, and how those assessments might be optimized.

The first of these watershed applications began in the late 1970s and continued through the 1980s, as the Central Intelligence Agency's (CIA) Directorate of Intelligence (the Agency's analytic arm) began circulating a series of internal documents "reviewing cognitive psychology literature concerning how people process information to make judgments on incomplete and ambiguous information" (Heuer 1999, p. vii). The research findings were digested and illustrated with challenges facing intelligence analysts, and accompanying recommendations for how analysts might apply evidence-based strategies to mitigate these common cognitive limitations. Many of these documents were authored by Richards Heuer, who subsequently compiled and supplemented them to create a now-classic work titled, *Psychology of Intelligence Analysis*. That body of work may represent the origins of "analytic science."

Heuer's memos described research illuminating a number of cognitive biases, limitations and heuristics (mental "shortcuts") that are common in nearly all forms of human judgment and decision-making. Among the points revealed in studies were:

- The human brain is "wired" to look for cause-and-effect explanations. As a result, people develop their own "mental models" of the problems they are trying to solve. Those models carry causal assumptions that may or may not have any basis in fact. Sometimes people are aware of their implicit models and assumptions; sometimes not. But those models and assumptions guide their judgments.
- Although people often think that having more information always leads to better decisions, studies suggest that is not true. There are limits to the value (or

"incremental validity") of adding new information. In fact, by always seeking "more information" people can add valueless inputs that ultimately undermine the accuracy of their decisions.

- When people are looking for answers or solutions under conditions of uncertainty, they tend to look for, and therefore find, information that confirms their prior assumptions and previously held beliefs. Information that does not fit with what they already believe is typically overlooked or dismissed. This creates an inherent "confirmation bias" in their judgments.
- Although people (including analysts) tend to value the forecasts of "experts" in a field much more than the predictions of people who do not have subject matter expertise, experts rarely produce more accurate predictive judgments—and sometimes they do significantly worse than non-experts. They certainly have no greater immunity to the general cognitive limitations and biases that routinely plague human decision making.

There are dozens of other known cognitive biases and heuristics that can affect decision making. The bad news is that it is probably impossible to eliminate them. The good news is, with awareness of these potential cognitive hazards, it may be possible to mitigate them or reduce their impact by changing the way a problem is structured or solved. The key implication, as Heuer points out, is that "Intelligence analysts should be self-conscious about their reasoning processes. They should think about *how* they make judgments and reach conclusions, not just about the judgments and conclusions themselves" (Heuer 1999, p. 31, emphasis in original). The highlights from these studies are still included in most intelligence analysis training programs.

Heuer's persistent interest in reducing bias and improving analytic judgments, led him (and other analysts, such as Randy Pherson) to develop a set of "Structured Analytic Techniques" (SATs). These are tools and techniques to help an analyst expose and explore her/his implicit mental model, to explore alternatives that may not comport with his/her prior beliefs, and to challenge her/his own conclusions and underlying arguments (Heuer and Pherson 2010). Although a given technique may serve multiple functions, they are generally grouped into three categories: *Diagnostic Techniques* aim to illuminate assumptions and make judgments more transparent; *Contrarian Techniques* challenge current thinking; and *Imaginative Thinking Techniques* are used to encourage new insights, perspectives or possible outcomes.

These techniques have become an essential part of intelligence analytic tradecraft taught within the U.S. Intelligence Community and in most analytic training programs. The SATs also cohere with and support the U.S. Intelligence Community's Analytic Standards, as outlined in Intelligence Community Directive 203 (ICD 203). The Analytic Tradecraft Standards described in ICD 203 require, among other things, that analytic products describe the underlying sources and methods used for the analysis; explicitly address any uncertainties; distinguish source information from assumptions and analytic judgments; and incorporate an analysis of alternatives. SATs hold substantial promise for improving the quality of analytic judgments and products. Unfortunately, despite SATs widespread inclusion in training

and policy, very little empirical research has been conducted to which ones work or when and how they may work (Artner et al. 2016).

The second major application of science to enhance human analytic performance—particularly for anticipatory analyses or forecasts—emerged through a program of research, funded by the Intelligence Advanced Research Project Activity (IARPA), called *The Good Judgment Project* (GJP). The GJP was a large scale, multi-year research study examining human judgments, individually and collectively, about geopolitical affairs and events—a task closely related to intelligence analysis, at least for National Intelligence. They used a "forecasting tournament" approach, logging hundreds of thousands of forecasts from over two thousand participants. The participants were not all political "experts," but those who signed up to participate did have higher levels of intelligence and political knowledge than the general population (Mellers et al. 2015).

The GJP research team wanted to understand what distinguished more accurate from less accurate forecasters, whether forecasters did better working on their own or in groups, and how the performance of aggregated ("crowdsourced") forecasts might differ from individual ones. A particularly intriguing question was whether training in probabilistic thinking, scenario analysis, and tips for mitigating cognitive bias could improve the accuracy of forecasts. The prediction questions pertained to events such as who would win an upcoming Russian election and whether a violent incident would occur in the South China Sea in 2013 that kills at least one person (Mellers et al. 2015; Ungar et al. 2012).

Concerning the question of what dispositional and behavioral characteristics might distinguish more accurate from less accurate forecasters, they found:

> *The best forecasters scored higher on both intelligence and political knowledge than the already well-above-average group of forecasters. The best forecasters had more open-minded cognitive styles. They benefited from better working environments with probability training and collaborative teams. And while making predictions, they spent more time deliberating and updating their forecasts* (Mellers et al. 2015, p. 10).

Regarding the question of whether forecasters did better working on their own or in groups, and how the performance of aggregated forecasts might differ from individual ones, GJP researchers found that team forecasts (where groups of forecasters discussed the questions collectively deliberated on them) and prediction markets (e.g., aggregated forecasts) performed better than individual ones, but that forecast accuracy varied depending on exactly *how* the collective forecasts were combined.

Characteristics of the Best Geopolitical Forecasters:

- Open-minded
- Good at pattern detection
- High cognitive flexibility
- Aware of their own biases

(continued)

- Good at inductive reasoning
- Good understanding of geopolitics
- Understand probabilistic reasoning
- Reflective and intellectually curious
- Understand the nature of uncertainty
- Put forth sustained effort in deliberations
- Perform successfully in team environments
- Continuously monitor ongoing current affairs
- View forecasting as a skill, not an innate "talent"
- Good at disaggregating and synthesizing problem components
- Committed to practice, learning from, and improving decisions
- Adjust their forecasts more regularly, based on changing circumstances
- Skilled in balancing factors that affect judgments (e.g., over-under confidence)

Source: Mellers et al. (2015), Tetlock and Gardner (2016) and Ungar et al. (2012).

Finally, the GJP Researchers found that training did improve the accuracy of predictions. That may seem intuitively obvious, but quite a few prior studies have found that training in statistics, for example, did not mitigate the common probability biases or misleading heuristics that commonly plague human judgments. People tend to underestimate and have lower confidence about high probability events (above .75), and to overestimate with higher confidence those events with low probability (below .75) (Ferrell 1994). Statistical training and education have not eliminated those tendencies, but the GJP training did seem to improve forecasters' accuracy (Chang et al. 2016).

The training evolved over the years of the study. The nature of the training, and lessons for aspiring forecasters, are described elsewhere in greater detail (Chang et al. 2016; Tetlock and Gardner 2016), but by Year 3, they were focusing on a set of tips for better probabilistic reasoning and a set of guidelines for political reasoning. As a mnemonic device, they represented the main points by the acronym: CHAMPS KNOW, which breaks down in the following way (Chang et al. 2016; Tetlock and Gardner 2016):

Probabilistic Reasoning Principles

- **C**omparison classes inform probability estimates
- **H**unt for the right information
- **A**djust and update forecasts when appropriate
- **M**athematical and statistical models can help
- **P**ost-mortem analysis after outcomes are known
- **S**elect the right questions to answer

Political Reasoning Principles:

- **K**now the power players and their preferences
- **N**orms and protocols of domestic and international institutions matter
- **O**ther perspectives (bottom-up eruptions of mass protest, globalization/interconnected-world arguments, efficient-markets thesis and its critics …) should also inform your forecasts
- **W**ildcards, accidents and black swans can catch you off-guard. Beware of irreducible uncertainty

Results from the Good Judgment Project represent some of the most significant applications science to advance human performance on intelligence-related analytic assessments.

1.3 Technology-Centered Advances in Intelligence Analysis

In the early days of intelligence analysis, finding "enough" data and information was an ongoing challenge. Today, we have the opposite problem – information overload. The volume, variety, and velocity of information continues to grow with no clear leveling point in sight. The devices we carry and use every day to work, to communicate and to entertain are continuously generating and emitting new data from text and images to radio frequency signals to GPS coordinates. And with a surge in the Internet of Things (IoT), we are adding new data-generating devices every day (Brantly 2018).

We have encountered data surges before in modern history; for example, when active communication satellites first appeared in 1962, but what we face today is truly unprecedented. Putting a number on that volume of data is nearly impossible. The numbers used to estimate it are almost incomprehensible. Just when people have gotten their heads around the idea of gigabytes and terabytes, the amount of information extends to petabytes (each is a thousand terabytes) and zettabytes (each is a billion terabytes). To illustrate the volume and velocity of data, a 2014 report by Dell EMC estimated the size of the "digital universe" in 2013 to be 4.4 zettabytes. The report predicted by 2020, its size would grow tenfold to 44 zettabytes (Dell EMC 2014). Collecting, storing, managing, and analyzing that amount of data poses a whole new set of challenges to law enforcement and intelligence agencies (Akhgar et al. 2015; Chan and Moses 2017). As a result, data literacy, management, and analysis are rapidly emerging as core competencies for intelligence analysts (Hare and Coghill 2016; Manning 2008; Ratcliffe 2004; Weston et al. 2019).

While the continued rise of "Big Data" poses a number of challenges for law enforcement organizations, it also offers some compelling opportunities. As ILP's popularity continues to grow, the availability of more data and the ability to aggregate and analyze that data greatly enhance the potential for "predictive policing" and multi-dimensional crime control methods, which is likely to lead to more science-informed operational planning (Leng and Li 2018). The emergent field of

"criminal analytics," based on Big Data, has important implications, not only for police patrols, but also for criminal investigation where tools may help to establish subject identities (resolving inconsistencies), reveal the structure of a criminal organization and the roles of its participants, link *modus operandi* across events, suggest subject location and profiles based on crime patterns and offense characteristics, and even shorten a list of suspects (Babuta 2017; Hu 2019; Li and Wang 2015; Perera et al. 2014; Pramanik et al. 2017).

In this section of the chapter, we will review some common and emergent technologies used by law enforcement intelligence professionals to exploit and derive insights from large amounts of data. Specifically, we will address spatial analytic technologies, network analytic technologies, data mining technologies, and the applications of artificial intelligence. These have been used in a wide range of policing applications, including human trafficking, wildlife trafficking, organized crime, and money laundering.

1.3.1 Spatial Analytic Technologies

Spatial analytic technologies have been a mainstay of crime analysis, almost since its inception. Spatial technologies, in the broadest sense, use place or location as the main unit of analysis. Before the advent of computer-assisted mechanisms, spatial analyses were manually represented on physical maps. It was an arduous, time-consuming process. These were the origins of "crime mapping." Early applications focused on the basic question of where, within a given jurisdiction, certain kinds of crimes were occurring. Because most crime in any given city is typically concentrated in 20% or less of the municipality's total area, this kind of mapping allowed police managers to allocate patrol resources where they were most needed.

Even when computerized crime mapping efforts first began to emerge in the late 1960s, however, the machinery was cumbersome and expensive and the results were very basic (akin to automated "pin mapping"). Crime mapping with Geographic Information Systems (GIS) did not really hit its stride until the late 1980s, as (a) information technologies advanced and became more affordable, (b) location-based crime reporting became mandatory, and (c) criminological approaches evolved from being offender-focused to more context-focused (Wang 2012).

The advent of the Global Positioning System (GPS) for geocoding markedly improved the accuracy and precision of GIS applications in law enforcement. In 1974, the US Government (USG) launched the first GPS satellite—part of its planned NAVSTAR System. The System currently has at least 32 operational satellites (with three "backups"), configured so that 24 are available 95% of the time. GPS was limited to military use until the early 1980s when it was opened to commercial civilian aircraft to improve safety and navigation. In 2000, Congress approved a plan to configure GPS satellites to transmit two additional signals that would be open for more widespread civilian use. Now, GPS receivers are inexpensive, widely available, and are even built into most smart phones. They are also commonly installed on police patrol vehicles and are increasingly attached to

equipment that officers carry on their persons. This has allowed law enforcement agencies to optimize their dispatching and to more closely track their officers in the field.

Law enforcement use of spatial technologies has expanded more recently into the use of unmanned aerial vehicles (UAVs or "drones"). Civilian UAV use became more popular after Congress passed the *FAA Modernization and Reform Act of 2012* (FAA Act), which effectively cleared drone use for policing operations. In a 2015 study of 46 law enforcement agencies in 11countries, more than a quarter (26%) said they were using UAVs for policing-related purposes (Custers and Vergouw 2015). GPS receivers are also embedded in many advanced UAVs. Civilian police drones are often equipped with cameras and may be used for static (crowds, objects, crime scenes) or dynamic observation (moving vehicles, suspects). Some drones, such as those configured with emitting light, sound or scent, even have the potential for "active" use on the public (Engberts and Gillissen 2016). The potential use of "armed" drones, either with lethal or "less lethal" armaments, by domestic, civilian law enforcement agencies remains a matter of active debate and discussion (Brumfield 2014; Straub 2014).

Law enforcement GIS applications are still primarily used for crime prevention and increasingly for criminal investigations. GIS has had a central role in "predictive policing," a term used to describe the practice of using spatio-temporal, historical data to anticipate or predict future crimes (Ferreira et al. 2012; Hardyns and Rummens 2018; Herchenrader and Myhill-Jones 2015). Location data are used (a) to identify "hotspots," which may be small geographic areas with high crime concentrations or areas where risk zones are more densely concentrated around particular criminal incidents, and (b) to create Risk Terrain Models to identify areas that are sensitive to higher crime rates (Hardyns and Rummens 2018). A rigorous review of 19 experimental or quasi-experimental evaluation studies found that hotspot policing led to significant reductions in crime and/or disorder in 20 of the 25 instances in which it was tested (Braga et al. 2012). Hotspot policing is widely regarded as one of the most robustly supported evidence-based policing and crime policy practices. Beyond GIS' broader function in identifying risk zones and hotspots for crime, geographic profiling has also assisted investigators in individual cases by identifying an offender's most likely area of residence based on the locations of a linked series of crimes (Rossmo 2012; Rossmo and Velarde 2008).

1.3.2 Network Analytic Technologies

Understanding criminal networks is extraordinarily important for exploiting criminal enterprises, and even assessing the behavior of particular criminal actors (Bichler 2019). The yields can be especially valuable to intelligence analysts, particularly in cases involving clandestine activity, complex criminal enterprises, or operational cells (Burcher and Whelan 2018; Sparrow 1991). Clark (2019) suggests that ignoring or under-analyzing network activity is one of the major causes of intelligence failures. Network analyses—basically a map of the ties and interactions among of

set of entities—have been successfully deployed in law enforcement against a wide range problems such as organized crime (van der Hulst 2009), drug trafficking (Bright et al. 2019), money laundering (Drezewski et al. 2015); terrorism (Dörfler et al. 2019); human trafficking, even trafficking wildlife (Haas and Ferreira 2015).

Different forms of network analysis exist. For example, basic Link Analysis and Analytic Charting have been staples in the analyst's toolkit for decades (Harper and Harris 1975). One of the most popular modern techniques among law enforcement and intelligence agencies has been Social Network Analysis (Van der Hulst 2009). About 43% of law enforcement agencies in one international sample said they employed SNA in their operations (Custers and Vergouw 2015). In SNA, people are typically the "entities" or "nodes" of interest. One key way in which SNA differs from other kinds of security-related analyses is that the focus is not on an individual offender, but on the ties and connections that each actor within a given system has or does not have with the other actors in that system. Simply put, relationships, not individual actors, are at the center of SNA (Van der Hulst 2009). Results are represented in visual form, which makes them easier for analysts to understand and to use in communicating network information to others (Xu and Chen 2005).

SNA reveals the structure of set of networked relationship. Analysts can interpret the implications of those structures for how the network will function and how its actors may behave (Custers and Vergouw 2015). Illicit and criminal networks do not always behave in the same way as legitimate and open networks (Bright et al. 2019). SNA can illuminate the roles and functions that actors may have in a network, and suggest important underlying dynamics like dependency between actors or relative power and position. It can visually represent and mathematically quantify the importance and centrality of the actors and the strength of ties between them (Bichler 2019; Jentner et al. 2018). SNA has been used successfully in law enforcement for scenario building, risk/threat assessments, hypothesis testing, network destabilization, and establishing identities in the presence of aliases and conflicting role information. Characterizing a criminal network in detail can even help intelligence planners in decisions about when, how, and where to deploy or insert human assets (Van der Hulst 2009).

1.3.3 Data Mining Technologies

Data mining is a broad term describing a range of tools and techniques for identifying patterns and extracting potential knowledge from large sets of data. Data mining techniques can be used for one or more of the following purposes: (1) to identify connections or associations between people or entities (Link Analysis, akin to SNA, which can be considered a Data Mining Technique); (2) to divide people or entities into clusters, classes, or categories; (3) to identify, define and describe concepts within a given knowledge domain; (4) to identify deviations or anomalies within data or data trends; and (5) to represent data visually to discern patterns and configurations that might not otherwise be detected in mathematical or numerical representations (Mishra and Shelke 2015).

These techniques have increasingly been applied in law enforcement contexts to support crime prevention, operational planning, and criminal investigations (McCue 2015; see Hassani et al. 2016 for an overview). Chen and colleagues (2003) provide the following examples of how various data mining techniques are used in policing:

> Entity extraction *has been used to automatically identify person, addresses, vehicles, narcotic drugs, and personal properties from police narrative reports.* Clustering techniques *such as "concept space" have been used to automatically associate different objects (such as persons, organizations, vehicles) in crime records.* Deviation detection *has been applied in fraud detection, network intrusion detection, and other crime analyses that involve tracing abnormal activities.* Classification *has been used to detect email spamming and find authors who send out unsolicited emails.* String comparators *have been used to detect deceptive information in criminal records.* Social network analysis *has been used to analyze criminals' roles and associations among entities in a criminal network" (pp. 1–2).*

There is substantial overlap between some data mining techniques and artificial intelligence (AI), primarily with regard to machine learning (ML). Machine learning is exactly what it sounds like. Algorithms are configured so that the software or "machine" actually learns as it sorts through the data. Two types of ML are commonly used, *supervised* and *unsupervised*. The difference pertains to whether the classification outcomes (or "ground truth") are known or unknown before the learning occurs.

For example, suppose you wanted to apply ML to distinguish fraudulent from legitimate account records. You could use supervised learning if you have a set of account records that you already know are fraudulent and a set that you know are not. The ML algorithms will examine all features or attributes of all accounts in the database (e.g., average balance, number of transactions in a given period, destinations of deposits, etc), compare those features between the two groups, "learn" which attributes differentiate those that are fraudulent from those that are legitimate, and build a model to predict the membership of new data points. If, however, you did not have a set of known fraudulent and legitimate accounts to start with, then the ML algorithms would need to sift through all attributes in all accounts to examine if two (or more) types of accounts could be identified based on the way the attributes cluster together or correlate with one another. If two (or more) clusters emerge from mining the data, then based on your prior knowledge (or what has been found in prior studies) and/or experience, you as the analyst would need to explore whether the way the attributes cluster and the differences between the two groups "make sense" or align with what might be expected in fraudulent and legitimate accounts. That would be an example of unsupervised learning. Although, in both cases, the software or machine learns from the data (learning is where the "intelligence" part of AI factors in), but what it learns, and how, is different.

Classification is one of the most fundamental and common uses for data mining and ML techniques. These techniques use rules or attributes within the data to sort entities into categories that are defined by those rules or attributes. In data mining, generally, there are three particularly common methods used for classification purposes: Decision Trees; Neural Networks; and Support Vector Machines. The following section discusses each of these in a bit more detail:

- **Decision Trees** use multistage algorithms (an algorithm is a formula that follows an established process or set of rules), ultimately leading to an endpoint outcome. The decision process is broken down into discrete segments, each with two or more options. Whichever of those options is selected or matched moves the formula to the next segment, that has two or more options. This process continues until the "answer" or ultimate outcome is reached. Decision Trees have been used to identify suspicious email messages and detect insurance fraud.
- **Artificial Neural Networks (ANNs)** comprise an interconnected set of component algorithms, modeled to function like the human brain, where each component (acting like a "processor") completes a small task that collectively contributes to the larger goal of recognizing a pattern. Typically, the network contains one or more "learning rules" that change the strength of the connection between components based on different inputs. ANNs do not process inputs in the logical, sequential way that typical serial computer processors do. The networks do not execute instructions; rather, they respond to the inputs based on the rules. These characteristics make ANNs especially useful when the relationships between variables are unknown or are complex and difficult to characterize. If the variables are *labeled*, the ANNs can classify them. If they are *unlabeled*, the ANNs can group or cluster them based on shared characteristics or attributes. "Through executing the learning process and using programmable memories, ANNs can predict new trends based on existing samples, and so they are being used to predict potential criminal patterns based on observations of current criminal activities" (Pramanik et al. 2017, pp. 5–6). ANNs have been applied to law enforcement tasks like detecting lies in a set of statements and identifying smuggling vessels.
- **Support Vector Machines (SVMs**) are often relatively simple algorithms used for supervised machine learning. Like all supervised learning, it begins with data from two known groups, from which it builds a model to predict group membership. Then the SVM sorts through the new data and classifies them into one of two groups or categories. The SVM's objective is to distinguish the two groups as clearly as possible, so that if they are plotted on a graph, the two clusters are visually as far apart from each other as possible. This can produce highly accurate results without requiring much computing power. SVMs can be used to categorize text, images, and even handwriting. SVMs have been applied in law enforcement tasks to identify harassing messages in social media posts, to identify the senders of emails and authors of documents, and for cybercrime detection.

1.3.4 Artificial Intelligence

Like Data Mining, the term Artificial Intelligence (AI) is used broadly to describe a wide range of computing technologies. A general definition might characterize AI as any software or hardware that either executes functions without human oversight or improves its own performance by learning from experience. The "intelligence" dimension refers to the ways in which AIs execute human-like tasks and functions,

thinking and acting rationally in perceiving, acting, learning, deciding and solving new problems (Hoadley and Lucas 2018). For law enforcement applications, AI systems have the potential to engage in surveillance, intelligence collection and analysis, and even direct enforcement actions. A common example of AI-driven enforcement might occur when cameras capture a vehicle that enters the plane of an intersection after the traffic light turned red, sends a message to an information system indicating that a violation has occurred involving a vehicle with a given registration tag; that system links the tag number to the registrant, and automatically generates a citation with a designated fine, which is sent to the vehicle's registrant. When no human intervention is involved in the process, the AI's actions are often referred to as "automated law enforcement" (Petit 2018).

Despite extraordinary investments and improvements in AI technologies, particularly over the past 15 years, the ability of automated systems to surveil, collect and analyze intelligence, and take responsive enforcement action is currently limited. The leaps in progress may be most evident in some intelligence collection and analysis tasks, where AI systems have information gathering and processing capabilities that often exceed those of their human counterparts (Allen and Chan 2017; Ganor 2019). AI's computing advantage does not suggest that law enforcement officers and intelligence analysts can or should be replaced by machines. Nor is that kind of replacement currently feasible or even likely to occur within the foreseeable future (Faizal Bin Abdul Rahman 2017).

As with any technology trend, the rise of AI poses new opportunities and new challenges. The trend for AI applications in law enforcement lies in identifying ways that computerized or automated capabilities can support and improve human decision making (Eldridge et al. 2018; Llinas et al. 2017; Pike 2019). Intelligence analysis continues fundamentally to be a human task, and there are compelling reasons in law enforcement applications to keep human analysts at the center of the process. New spatial, network and data analytic technologies, however, can bring more data and different kinds of data to bear on critical decisions and strengthen the evidence base for analytic assessments. Algorithms and machine learning may be important components of that process (Regens 2019).

Analytic and AI technologies may be evolving to a point where they might effectively serve as consultants to investigators and analysts (Tecuci et al. 2014). "Intelligent agents" are a major focus area in AI research. The term does not refer to intelligence officers, assets or agents. The "agency" lies within the software or hardware itself. According to Brenner and colleagues (Brenner et al. 2012) "intelligent software agents are defined as being a software program that can perform specific tasks for a user and possesses a degree of intelligence that permits it to perform parts of its tasks autonomously and to interact with its environment in a useful manner" (p. 21). These agents can identify, extract and monitor information for analysis and potentially for response (Brenner et al. 2012). This kind of automated action could provide invaluable support for law enforcement intelligence analysts.

Although the abilities of AI technologies to classify and predict are constantly improving, data mining and AI technologies are quite limited when it comes to "understanding" phenomena and determining causal relationships. They may

predict an outcome with reasonable accuracy, but they cannot explain why that decision was reached. While AI and data analytics can enable and accelerate LE analytic capabilities, humans infuse meaning and sense making into the results (Lim 2016). Data mining and AI may best support human analysts by triaging large volumes of data and extracting key elements to hone the analyst's focus (Llinas et al. 2017). Of course, to properly leverage (and contain) these technologies, proficiencies in data science and technology are likely to become increasingly important skills for law enforcement intelligence analysts (Eldridge et al. 2018).

2 Conclusions

Intelligence-led policing has become a popular, in some cases even dominant, approach to managing law enforcement operations in many Western countries (Bureau of Justice Assistance 2005; Ratcliffe 2016). This philosophical shift has elevated the importance of intelligence analytic capabilities in police organizations, and put intelligence analysts at the center of critical operational decisions (Burcher and Whelan 2019). Over the past 20 years, trends in professionalism and professional standards within the field of law enforcement intelligence analysis, and external developments in science and technology have considerably advanced analytic practice.

Looking at the human side of scientific advances, the emergence of two major professional organizations—IALEIA and IACA—have moved law enforcement analysts toward a sense of collective identity and created an infrastructure to improve both analyst qualifications and analytic products. Although each organization has a slightly different analytic focus (traditional vs data-driven analytic tradecraft) both offer analytic training, have the reference sources for a common body of knowledge, and have established professional certification programs. Also, cognitive psychologists have been giving greater attention to researching analytic tasks, and intelligence analysts have been following that research more closely and applying it to their own tradecraft. A very recent scientific research program—the Good Judgment Project—has begun to illuminate "what works" in forecasting future (particularly geopolitical) events, and the kind of traits and abilities that characterize people who consistently make the most accurate predictions. This cross-pollination of science and practice may lead to greater reliance on science-informed intelligence analysis in policing.

On the technological side of advances in the field, a range of data analytic technologies have emerged to help analysts manage the influx of Big Data. Spatial technologies can identify location patterns among people, objects or events. Network analyses can illuminate how people, objects or events are connected or tied together. Data Mining technologies can find patterns and anomalies amidst massive volumes of structured or unstructured data. And Artificial Intelligence technologies can learn from sifting through datasets; can cluster, classify or categorize the data; and can identify the more reliable and relevant data points, reducing the data load for

analysts. Machine-driven analytic technologies will continue to improve, and will likely do so at an incredible pace. Their applications in law enforcement operations will test legal, ethical and policy boundaries, but they cannot and will not replace critical capabilities provided by trained human analysts.

References

Ackoff, R. L. (1989). From data to wisdom. *Journal of Applied Systems Analysis, 16*(1), 3–9.

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (2015). *Application of big data for national security: A practitioner's guide to emerging technologies*. Waltham: Butterworth-Heinemann.

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security* (Vol. 132). Cambridge, MA: Belfer Center for Science and International Affairs.

Artner, S., Girven, R. S., & Bruce, J. B. (2016). *Assessing the value of structured analytic techniques in the US intelligence community* (No. RR-1408-OSD). Santa Monica: RAND National Defense Research Institute.

Babuta, A. (2017). Big data and policing: An assessment of law requirements, expectations and priorities. In *RUSI occasional paper*. London: Royal United Services Institute for Defence and Security Studies. Retrieved from https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

Bichler, G. (2019). *Understanding criminal networks: A research guide*. Oakland: University of California Press.

Braga, A., Papachristos, A., & Hureau, D. (2012). Hot spots policing effects on crime. *Campbell Systematic Reviews, 8*(8), 1–96.

Brantly, A. F. (2018). When everything becomes intelligence: Machine learning and the connected world. *Intelligence and National Security, 33*(4), 562–573. https://doi.org/10.1080/02684527.2018.1452555.

Brenner, W., Zarnekow, R., & Wittig, H. (2012). *Intelligent software agents: Foundations and applications*. New York: Springer Science & Business Media.

Bright, D., Koskinen, J., & Malm, A. (2019). Illicit network dynamics: The formation and evolution of a drug trafficking network. *Journal of Quantitative Criminology, 35*(2), 237–258.

Bruce, J. B., & George, R. (2015). Professionalizing intelligence analysis. *Journal of Strategic Security, 8*(3), 1–23.

Brumfield, E. (2014). Armed drones for law enforcement: Why it might be time to re-examine the current use of force standard. *McGeorge Law Review, 46*, 543–572.

Burcher, M., & Whelan, C. (2018). Social network analysis as a tool for criminal intelligence: Understanding its potential from the perspectives of intelligence analysts. *Trends in Organized Crime, 21*(3), 278–294. https://doi.org/10.1007/s12117-017-9313-8.

Burcher, M., & Whelan, C. (2019). Intelligence-led policing in practice: Reflections from intelligence analysts. *Police Quarterly, 22*(2), 139–160. https://doi.org/10.1177/1098611118796890.

Bureau of Justice Assistance. (2005, September). *Intelligence-led policing: The new intelligence architecture*. Washington, DC: Bureau of Justice Assistance. Retrieved from: https://www.ncjrs.gov/pdffiles1/bja/210681.pdf

Carter, D. L. (2009). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies*. Washington, DC: US Department of Justice, Office of Community Oriented Policing Services.

Carter, D. L., & Carter, J. G. (2009). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review, 20*(3), 310.

Chan, J., & Moses, L. B. (2017). Making sense of big data for security. *British Journal of Criminology, 57*(2), 299–319. https://doi.org/10.1093/bjc/azw059.

Chang, W., Chen, E., Mellers, B., & Tetlock, P. (2016). Developing expert political judgment: The impact of training and practice on judgmental accuracy in geopolitical forecasting tournaments. *Judgment and Decision making, 11*(5), 509–526.

Chen, H., Chung, W., Qin, Y., Chau, M., Xu, J. J., Wang, G., Zheng, R., & Atabakhsh, H. (2003, May). Crime data mining: an overview and case studies. In *Proceedings of the 2003 annual national conference on Digital government research* (pp. 1–5). Digital Government Society of North America.

Clark, R. M. (2019). *Intelligence analysis: A target-centric approach (6th Ed.)*. Washington, DC: CQ Press.

Custers, B., & Vergouw, B. (2015). Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies. *Computer Law & Security Review, 31*(4), 518–526.

Dell EMC. (2014). *The digital universe of opportunities: Rich data and the increasing value of the internet of things*. Hopkinton: Dell EMC.

Dörfler, T., Stollenwerk, E., & Schibberges, J. (2019). *Uncovering covert structures: Social network analysis and terrorist organizations*. London: SAGE.

Drezewski, R., Sepielak, J., & Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences, 295*, 18–32. https://doi.org/10.1016/j.ins.2014.10.015.

Eldridge, C., Hobbs, C., & Moran, M. (2018). Fusing algorithms and analysts: Open-source intelligence in the age of 'Big Data'. *Intelligence and National Security, 33*(3), 391–406. https://doi.org/10.1080/02684527.2017.1406677.

Engberts, B., & Gillissen, E. (2016). Policing from above: Drone use by the police. In B. Custers (Ed.), *The future of drone use* (pp. 93–113). The Hague: TMC Asser Press.

Faizal Bin Abdul Rahman, M. (2017). Why it won't displace police analysts artificial intelligence. *RSIS Commentary, 109*, 1–3.

Ferreira, J., João, P., & Martins, J. (2012). GIS for crime analysis: Geography for predictive models. *Electronic Journal of Information Systems Evaluation, 15*(1), 36.

Ferrell, W. R. (1994). Discrete subjective probabilities and decision analysis: Elicitation, calibration and combination. In G. Wright & P. Ayton (Eds.), *Subjective probability* (pp. 411–451). Chichester: Wiley.

Ganor, B. (2019). Artificial or human: A new era of counterterrorism intelligence? *Studies in Conflict and Terrorism, 0*(0), 1–20. https://doi.org/10.1080/1057610X.2019.1568815.

Gentry, J. A. (2016). The "professionalization" of intelligence analysis: A skeptical perspective. *International Journal of Intelligence and CounterIntelligence, 29*(4), 643–676.

Global Justice Information Sharing Initiative. (2003). *The national criminal intelligence sharing plan*. Washington, DC: Global Justice Information Sharing Initiative, U.S. Department of Justice.

Global Justice Information Sharing Initiative. (2007). *Law enforcement analyst certification standards*. Washington, DC: Global Justice Information Sharing Initiative, U.S. Department of Justice.

Haas, T. C., & Ferreira, S. M. (2015). Federated databases and actionable intelligence: Using social network analysis to disrupt transnational wildlife trafficking criminal networks. *Security Informatics, 4*(1), 1–14. https://doi.org/10.1186/s13388-015-0018-8.

Hardyns, W., & Rummens, A. (2018). Predictive policing as a new tool for law enforcement? Recent developments and challenges. *European Journal on Criminal Policy and Research, 24*(3), 201–218. https://doi.org/10.1007/s10610-017-9361-2.

Hare, N., & Coghill, P. (2016). The future of the intelligence analysis task. *Intelligence and National Security, 31*(6), 858–870. https://doi.org/10.1080/02684527.2015.1115238.

Harper, W. R., & Harris, D. H. (1975). The application of link analysis to police intelligence. *Human Factors, 17*(2), 157–164.

Harrison, M., Walsh, P. F., Lysons-Smith, S., Truong, D., Horan, C., & Jabbour, R. (2018). Tradecraft to standards—Moving criminal intelligence practice to a profession through the

development of a criminal intelligence training and development continuum. *Policing: A Journal of Policy and Practice*, 1–13. https://doi.org/10.1093/police/pay053.

Hassani, H., Huang, X., Silva, E. S., & Ghodsi, M. (2016). A review of data mining applications in crime. *Statistical Analysis and Data Mining: The ASA Data Science Journal, 9*(3), 139–154.

Herchenrader, T., & Myhill-Jones, S. (2015). GIS supporting intelligence-led policing. *Police Practice and Research, 16*(2), 136–147.

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.

Heuer, R. J., & Pherson, R. H. (2010). *Structured analytic techniques for intelligence analysis*. Washington, DC: CQ Press.

Hoadley, D. S., & Lucas, N. J. (2018). *Artificial intelligence and national security*. Washington, DC: Congressional Research Service.

Hu, J. (2019). Big data analysis of criminal investigations. In *2018 5th international conference on systems and informatics, ICSAI 2018* (pp. 649–654). https://doi.org/10.1109/ICSAI.2018.8599305.

Jentner, W., Sacha, D., Stoffel, F., Ellis, G., Zhang, L., & Keim, D. A. (2018). Making machine intelligence less scary for criminal analysts: Reflections on designing a visual comparative case analysis tool. *The Visual Computer, 34*(9), 1225–1241. https://doi.org/10.1007/s00371-018-1483-0.

Leng, J., & Li, G. (2018). Big data-driven predictive policing innovation. *Advances in Engineering Research, 163*, 123–127. https://doi.org/10.2991/iceesd-18.2018.19.

Li, J., & Wang, A. G. (2015). A framework of identity resolution: Evaluating identity attributes and matching algorithms. *Security Informatics, 4*(1). https://doi.org/10.1186/s13388-015-0021-0.

Lim, K. (2016). Big data and strategic intelligence. *Intelligence and National Security, 31*(4), 619–635.

Llinas, J., Rogova, G., Barry, K., Hingst, R., Gerken, P., & Ruvinsky, A. (2017). Reexamining computational support for intelligence analysis: A functional design for a future capability. *Autonomy and Artificial Intelligence: A Threat or Savior?* (April 2018), 13–46. https://doi.org/10.1007/978-3-319-59719-5_2

Manning, P. (2008). *The technology of policing: Crime mapping, information technology, and the rationality of crime control*. New York: New York University Press.

Marrin, S. (2016). Improving intelligence studies as an academic discipline. *Intelligence and National Security, 31*(2), 266–279.

Marrin, S., & Clemente, J. D. (2006). Modeling an intelligence analysis profession on medicine. *International Journal of Intelligence and CounterIntelligence, 19*(4), 642–665.

McCue, C. (2015). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Oxford/Waltham: Butterworth-Heinemann.

Mellers, B., Stone, E., Atanasov, P., Rohrbaugh, N., Metz, S. E., Ungar, L., Bishop, M., Horowitz, M., Merkle, E., & Tetlock, P. (2015). The psychology of intelligence analysis: Drivers of prediction accuracy in world politics. *Journal of Experimental Psychology: Applied, 21*(1), 1–14.

Mishra, N., & Shelke, P. (2015). Data mining – A necessity for crime detection. *International Journal on Recent and Innovation Trends in Computing and Communication, 3*(2), 291–294. Retrieved from http://www.ijritcc.org

Perera, H., Udeshini, S., & Munasinghe, M. (2014, November). *Criminal short listing and crime forecasting based on modus criminal short listing and crime*. https://doi.org/10.13140/RG.2.1.5149.1287

Petit, N. (2018). Artificial intelligence and automated law enforcement: A review paper. *SSRN Electronic Journal, 1*(1974), 1–12. https://doi.org/10.2139/ssrn.3145133.

Pike, T. (2019, May). *Computational tools to support analysis and decision making*, 23. https://doi.org/10.1117/12.2518693.

Pramanik, M. I., Lau, R. Y. K., Yue, W. T., Ye, Y., & Li, C. (2017). Big data analytics for security and criminal investigations. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(4), 1–19. https://doi.org/10.1002/widm.1208.

Ratcliffe, J. H. (2004). Crime mapping and the training needs of law enforcement. *European Journal on Criminal Policy and Research, 10*(1), 65–83.

Ratcliffe, J. (2016). *Intelligence-led policing*. New York: Routledge.

Regens, J. L. (2019). Augmenting human cognition to enhance strategic, operational, and tactical intelligence. *Intelligence and National Security, 34*(5), 673–687. https://doi.org/10.1080/02684527.2019.1579410.

Rossmo, D. K. (2012). Recent developments in geographic profiling. *Policing: A Journal of Policy and Practice, 6*(2), 144–150.

Rossmo, D. K., & Velarde, L. (2008). Geographic profiling analysis: Principles, methods and applications. In S. Chainey & L. Thompson (Eds.), *Crime mapping case studies: Practice and research* (pp. 35–43). New York: Wiley.

Rowley, J. (2007). The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163–180.

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*(3), 251–274.

Straub, J. (2014). Unmanned aerial systems: Consideration of the use of force for law enforcement applications. *Technology in Society, 39*, 100–109.

Tecuci, G., Schum, D. A., Marcu, D., & Boicu, M. (2014). Computational approach and cognitive assistant for evidence-based reasoning in intelligence analysis. *International Journal of Intelligent Defence Support Systems, 5*(2), 146. https://doi.org/10.1504/ijidss.2014.059976.

Tetlock, P. E., & Gardner, D. (2016). *Superforecasting: The art and science of prediction*. London: Random House.

Ungar, L., Mellers, B., Satopää, V., Tetlock, P., & Baron, J. (2012, October). *The good judgment project: A large scale test of different methods of combining expert predictions*. AAAI technical report FS-12-06: Machine Aggregation of Human Judgment, 37–42.

Van der Hulst, R. C. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. *Trends in Organized Crime, 12*(2), 101–121. https://doi.org/10.1007/s12117-008-9057-6.

Wang, F. (2012). Why police and policing need GIS: An overview. *Annals of GIS, 18*(3), 159–171.

Warner, M. (2002). Wanted: A definition of "intelligence". *Studies in Intelligence, 46*(3), 15–22.

Weston, C., Bennett-Moses, L., & Sanders, C. (2019). The changing role of the law enforcement analyst: Clarifying core competencies for analysts and supervisors through empirical research. *Policing and Society*. https://doi.org/10.1080/10439463.2018.1564751.

Xu, J., & Chen, H. (2005). Criminal network analysis and visualization. *Communications of the ACM, 48*(6), 100–107.