Jerome, Barlatier

Article

Criminal investigation and criminal intelligence: Example of adaptation in the prevention and repression of cybercrime

Risks

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Jerome, Barlatier (2020) : Criminal investigation and criminal intelligence: Example of adaptation in the prevention and repression of cybercrime, Risks, ISSN 2227-9091, MDPI, Basel, Vol. 8, Iss. 3, pp. 1-10, https://doi.org/10.3390/risks8030099

This Version is available at:
https://hdl.handle.net/10419/258052

risks

MDPI

Article

Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime

Barlatier Jerome

Head of Criminal Intelligence Division in French National Gendarmerie-PONTOISE (95), 95000 Pontoise, France; jerome.barlatier@gendarmerie.interieur.gouv.fr

Received: 23 April 2020; Accepted: 15 September 2020; Published: 18 September 2020

Abstract: In the context of the digitization of delinquent activities, perpetrated via the internet, the question of the most appropriate means of crime prevention and crime repression is once again being raised. Studies performed on police investigations have highlighted the over-determining nature of circumstantial factors in crime as a condition for their elucidation for more than fifty years. The emergence of mass delinquency, such as cybercrime, has thus strongly altered the role of investigation as a useful mode of knowledge production. This obsolescence has appeared gradually and can be summarized in four stages, which generates a suspicion about the social relevance of the investigation. It seems that the holistic approach of criminal intelligence is more adapted to the fight against new forms of crime. The investigation becomes a precision instrument assigned to functions that become more specific. This article considers this paradigm shift by the approaches to knowledge management of crime control. Cybercrime is then emblematic of this shift. This study is based on the criminological review and the delinquency analysis led by the central criminal intelligence service of the national gendarmerie. Its premise may likely guide the strategy of French law enforcement agencies.

Keywords: criminal investigation; criminal intelligence; intelligence-led-policing; risk society

---

The response to crime reveals how the society treats the just and the unjust, the legitimate and the illegitimate. These dualities seem to have been governed by the distinction between right and wrong for a long time. What is true? Who has the right to define it? Based on which technique of knowledge? How is it perceived?

The prerogative to tell the truth, to concretize it through a technique of knowledge, and it is commonly considered as such, has been the main link of power for long. It is based on "truth games" and "knowledge effects" that shape and organize a distribution of the world on which justice is based (Foucault 1972). The political authorities decide on criminal sanctions through their attention and effectiveness in dealing with certain illegal behaviors that they consider as major threats, and the justice separates the true from the false, the legal from the illegal.

In this logic, Michel Foucault reminds us that the criminal justice system, as we understand, has not always been like this. For the historian-philosopher, the truth is a social construct that has undergone a long process of maturation per stages where "the test", i.e., the determination of the truth by arbitrary confrontation asserting the right to be true; "the proof", i.e., the repressive investigation based on the reconstitution of facts by reason; "the examination", i.e., preventing dangerousness by science; and finally "the measure", i.e., ordering of risks by evaluated categories establishing a just order by means of the exact sciences.

According to Foucault, investigation and examination are technologies of power and control. While the former is fact-oriented and the latter is person-oriented, both express a desire for control at the individual level and for the customized measures. It is by practicing power over everyone that we can govern them all. Measurement, on the other hand, has a holistic value and seeks to apply

standards to individuals. Foucault thus marks many shifts in the mechanisms of social regulation, from a violent, visible, and individual sanction to a diffuse and collective disciplinary action, from a reaction of crime (i.e., investigation, materializing the circumstances of a past crime) to the scientific anticipation of its risk factors (i.e., the evaluation of a criminal's future dangerousness).

British criminologist Lucia Zedner (2007) proposes a similar distinction by noting the transition from a "pre-crime" to a "post-crime" society. She thus confirms the emergence of a society based on risk prevention, where the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime aspect of security. Crime is no longer seen as an evil, but as a risk. Damage is experienced as a potential loss that must be avoided at best and compensated at worst. This pre-criminal logic is based on the risk calculation, the control of unpredictabilities, the surveillance, the precaution, and the prevention. It is followed by an increasing privatization, which transforms the security into a market value. Moving its gravity center from the "after" to the "before" crime, it seeks to reduce opportunities, and to target and to increase surveillance based on prudentialism and actuarialism. The individual attention to the offender is supplanted by the risk management of these "dangerous classes". The insurance welfare system, on the other hand, pools risks and losses.

Such emergence has taken place by a deconstruction of the social landmarks in the post-modernist era. The social, professional, economic, or geographical mobility of populations has promoted anonymity and weakened the traditional frameworks of social control. French philosopher Gilles Lipovetsky notes that the first values of liberation and optimism promoted by post-modernism have started to fade in favor of a generalized demand for protection (Lipovetsky and Charles 2004). The weakened traditional social regulators (i.e., justice) have been then replaced by a new mode of regulation based on risk management.

In this risk society, it is better to control the present and future than to focus the energy on the resolution of past situations.

The investigation is a rational process of information management in order to contribute to the truth established in Court. It works on the opposite side of the risk society values. It must adapt to this new context to prevent from becoming an obsolete means for social regulation (Barlatier 2017). This article presents an evolution of concepts that could help to overcome this obsolescence—from the manifestation of the truth about the crime to the management of risks related to the delinquency, from the use of judicial investigation to the use of criminal intelligence. Cybercrime is an important framework of this transition.

1. From the Manifestation of Truth to Risk Management

1.1. Modern Investigation and Disclosure of Evidence

Formally appearing in the 18th century, the investigation promotes the Enlightenment movement and plans to produce knowledge by rational processes. Issues both from private and public activities, the investigations of the detective and the police officer were initially based on the knowledge and infiltration of a criminal environment. The positivist movement and the industrial revolution then made the emergence of the "scientific" investigation possible, out of scorias of compromise. In the twentieth century, the investigation takes advantage from the major management concepts to structure itself, to standardize the processes, and to increase the performance of its action.

Nevertheless, the investigation keeps its core purposes—to reconstruct the past for the justice to do its work.

Whatever the data source (forensics, testimonies, observations, or digital logs), the investigation collects the data by graduated levels of presumption under the triptych format suspicion–evidence–proof. The investigator relies first on legal reasoning. They collect the elements with the purpose of identifying the perpetrator under the law. Then, they characterize the offence with proofs, which are considered as sufficient by the judges. Understanding the crime and its motivation is not a priority. The investigation is governed by the what and the who; the how and the why are only explored if they

serve the first two. For instance, a homicide requires a knowledge of the perpetrator's motives and an understanding of the circumstances of the crime, whereas a supermarket shoplifting investigation does not need to know the context of the offence. A simple material finding of the facts is usually sufficient. However, these acts of low-intensity delinquency may be committed in a serial manner, within a framework of structured criminal organizations, and causes serious damage to businesses.

Investigation is thus an art of individualizing the link between the criminal act and the perpetrator for judicial purposes. It is led by a procedural framework that ensures a compromise between crime control and due process.

Motivated by the high moral value of not allowing crime to go unpunished, guided by the ideal of truth, and oriented towards the repressive purpose of a customized criminal sanction, the investigation underpins a separation of powers, where the State, in a regalian approach, has the monopoly of coercion and where justice, in a balance of powers, guarantees individual freedoms.

The traditional system of this rational judicial investigation has functioned consistently for almost a century, adapting to its environment, specifically to the increase of the crimes through a delegation system from the magistrate to the police officer.

Four suspicions are gradually challenging its effectiveness as a process of knowledge production and of social regulation from a Foucauldian point of view (Barlatier 2019).

The first suspicion appears with the strong growth of thefts that ensues the development of consumer goods from the end of the 19th century onwards. We face an increasing mobile and anonymous predation that investigation struggles to handle. Thefts, specifically burglaries and car thefts, are well reported by the victims (90% of car thefts and 75% of burglaries are the subject of a complaint (ONDRP 2019)). Both the elucidation of these acts and its penalization are relatively low due to its usual and serial characteristics.

The second suspicion appears with the development of white-collar crime. By a reactive position (i.e., action at the moment of the citizen complaint), the law enforcement agencies are struggling to apprehend this form of crime without a direct victim as a good knowledge of the company environment and the management of both complex and technical litigation are required. Turning away from recourse to the court of justice, the markets and economic institutions are developing other forms of regulation, creating a biotope favorable to social control (contractualization of relations or control of competition and prices, for example). In this context, recourse to the criminal courts is only an ultima ratio, a subsidiary mode of managing litigation.

The third suspicion arises with the development of the illicit economic market in drug trafficking in the 1960s and 1970s. The law enforcement agencies and the judicial system then witnessed the emergence of a new phenomenon that they were likely to control ab initio. Drug trafficking is one of the most lucrative economic activities fifty years later and could not be stopped. The investigation has once again proved irrelevant to counter this phenomenon.

The fourth suspicion comes with the internet. The law enforcement agencies are working on its impact related to crime and criminal response in the late 1990s and early 2000s. In terms of damage to property, the recent studies compare the same volume between cybercrime and physical crime (Loveday 2018). At the same time, victims no longer consider the police as a solution. The dark figure represents 99.5% for some categories of offences committed on the internet (Dregoir and Edouard 2017). The crime-solving rate is also particularly low, specifically for scams, which are more than 70% of offences detected in cyberspace. Faced with this massive and international phenomena generating technical and arid litigation, the investigation becomes obsolete and is not able to meet the major challenges of crime (source: study of complaints filed from 2015 to 2020—Criminal Intelligence Service—Gendarmerie Nationale).

Cybercrime is approached in a traditional way without any consideration of societal changes. Any cyber complaint is managed by any isolated investigator who is not well trained on the cyber high technicality of investigations. Indeed, investigative measures consist of requesting information from operators, who used to be uncooperative, in order to have access to data, which are most of the

time located abroad. The complexity of the international cooperation procedures is disproportionate related to the handling of massive litigation involving small and medium-scale delinquency. Moreover, the outcome is often uncertain, and this treasure hunt rarely succeeds in lifting the anonymity of the perpetrators, as the countermeasures are many and common (use of virtual private network—VPNs, use of false identities, etc.). Each fact is addressed per unique victim, and so the lack of connection between cases usually prevents the phenomena from being considered in their true extent. Therefore, the accumulation of small prejudices for the victims is not translating into a significant criminal benefit for the perpetrators. Besides, attempting to demonstrate a criminal series used to end with a difficult case to manage in proceedings, due to the multiplicity of victims and the complexity of providing simple and intelligible evidence to the judge.

1.2. Post-Modern Investigations and Risk Assessment

Starting in the second half of the 20th century, the political implementation of ideologies has ruined the rationalism and positivism that had prevailed for two centuries. Modernism is replaced by a post-modern era that is nourished by relativism. It is marked by a collapse of traditional collective frameworks (specifically with the loss of the states' influence through both internationalization and the decentralization) and by a fragmentation of social and individual identities (emergence of multiple identities, restructuring of families, multiple membership of social groups) (Reiner 1992; Brodeur 1993). The decline of political, economic, and social benchmarks leaves each one to his or her own responsibility. An individual is subjected to uncertainty, develops a feeling of insecurity, and tries to adapt through risk management approaches (Lipovetsky and Charles 2004).

This paradigm shift has an effect in criminological terms (Reiner 1992). It leads to an evolution of social regulation processes and to a questioning of the action modes on criminal justice: "*comment redéfinir une justice pénale fondée sur la notion de responsabilité individuelle, de façon qu'elle puisse faire face au caractère systémique des problèmes qui lui sont soumis et qu'elle parvienne à gérer les collectivités qui constituent sa clientèle, sans renoncer au respect des droits de la personne?*[1]" (Brodeur 1993, p. 52). Three issues of this evolution are then considered to overcome the contradiction between penal individualism and the massive delinquency—the creation of a new penology focused on post-penal follow-up of convicted offenders in an open environment, a hybridization between the public and private sectors for a better control of the public area, and a dilution of the offence focused on the repression of individuals rather than on the criminalization of facts (Ibid.).

The criminal justice system is thus challenged on its three pillars of legality, individualization, and territoriality. It leads to an internationalization of procedures and a disruption of the criminal actors. It leads both to a neo-positivism (the right to forget is being eroded, the introduction of a system for anticipating danger, and monitoring convicted persons) and to a new penal utilitarianism (i.e., a public management policy seeking greater efficiency) (Massé et al. 2009).

These developments provide fertile ground for the emergence of a risk-based approach to crime. "*Le risque est un danger sans cause, un dommage sans faute, qui pourtant devient prévisible et calculable*[2]" (Peretti-Watel 2001, p. 6).

Thus, a true prudential logic takes place, based on the expert diagnostic and public opinion. The aim is no longer to determine the criminal responsibility of the perpetrator for a past offence, but to reduce the uncertainty of the present and the future by calculating the probabilities of risk with the actuarial method. Crime thus loses its specificity and becomes an ordinary social risk, just like unemployment, poverty, technological accidents, natural disasters, or epidemiological risks. As a result, the concepts of criminal responsibility and guilt are no longer linked. By the risk approach, the

---

[1] How can criminal justice be redefined based on the notion of individual responsibility, so that it can deal with the systemic nature of the problems submitted to it and manage the communities that constitute its clientele, without abandoning respect for human rights?

[2] Risk is a danger without cause, a damage without fault, which nevertheless becomes predictable and calculable.

offence is an accident and the person responsible is no longer guilty (L'Heuillet 2001). This is how Lucia Zedner concludes on the transition from a post-crime society to a pre-crime society.

There is thus a real paradigmatic break between the rationalism of the modern era and the relativism of the post-modern era. If the former claimed to access the truth through justice, the latter is satisfied by reducing uncertainty through risk management, as shown in Figure 1.

Modernism	Risk Society
Legitimacy	Effectiveness
Policy	Management/Regulation
Governing	Governance
Moralism	Relativism
Truth in progress	Disenchantment
Reason	Adaptation
Realism and Truth	Predictabilities of results
Legality	Risk Management
Repression	Problem solving

Figure 1. Paradigm shift between modern society and the risk society (source: Barlatier 2017, p. 48).

According to some researchers, the police forces try to adapt to these new challenges through four evolutions: massification, judiciarization, technologization, and multilateralization (Jobard and de Maillard 2015). Over the last fifty years, they obviously tried to go beyond the reactive framework to implement more proactive strategies by strengthening their feet (community policing—COP, Skogan 2004), their arms (problem-oriented policing—POP, Goldstein 1990), or their heads (intelligence-led policing—ILP, Ratcliffe 2016). The increase of the management of services (e.g., Compstat in New York, Bratton 1998) has strengthened the planning and control of the police activities, and in parallel, to increase the efficiency. The police force moves away from its administrative and bureaucratic functioning (Bitner 1970) to become a policy, sometimes focused on proximity, sometimes on intervention, sometimes on intelligence.

Over the last 20 years, many States have based their security policy on the ILP and have developed a criminal intelligence system designed to guide police action (e.g., the British National Intelligence Model—NIM, Home Office 2010). If the strategic framework allows the understanding of phenomena, an operational framework helps the operational managers to make decisions, the same as a tactical framework for the investigators. The criminal intelligence is dedicated to play a central role in the operation of the police system by increasing the relevance of its diagnostics and measures to remedy crime (Ratcliffe 2016). The investigation is then placed at the service of intelligence. The investigation contributes to understanding phenomena and criminal gangs through case studies, and the intelligence apprehends them globally through a broader data collection, a processing of information more demanding and some solutions more diversified.

In this way, criminal intelligence is part of genuine risk management where the objective is not to find the truth, but to reduce uncertainty in an imperfect information environment. We are moving from an event-centered logic, characteristic of the investigation, to a suspect-centered logic. The police concentrate their action on the minority of the population that has chosen delinquency as a way of life. This approach is necessary to break down the traditional compartmentalization between security and justice actions inherited from the separation of administrative and judicial powers. It encourages the

establishment of a continuum between these two poles as described on the following cycle, as shown in Figure 2.

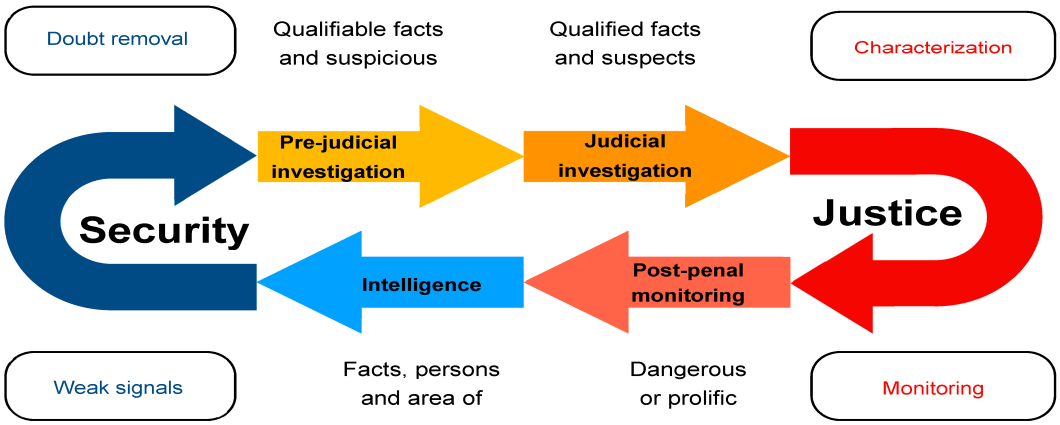

Figure 2. Continuity of information processing between security action and justice action (adapted from Barlatier 2017, p. 287).

Following many terrorist attacks, the law tends to give an equivalence power to security and justice action, thus upsetting the traditional balance between crime control and due process.

There is therefore a shift in the notions of investigation and intelligence, which marks an evolution in police action, as shown in Figure 3.

Investigation	Intelligence
Reconstructing the past to tell the truth	Anticipating the future through the probable
Rationality and reliability of evidence, moral value	Evolution in an environment of post-truth, relativism, economic value
Fighting injustice	Do not waste time
Casuistic approach	Holistic approach
Investigation with a judicial purpose	Intelligence with a security purpose
Penal repression	Social regulation
Separation of powers	Security/justice continuum
Regalian approach to security and justice	Public-private hybridization
Evidence-based approach	Risk-based approach
Judicial authorization for infringements of individual liberties	Granting of investigative powers to the administration within the framework of its intelligence mission
Police monopoly of the investigation	Sharing the investigation with the private sector
Procedural action based on securing rights through the validity of the procedure	Processual action oriented on framework efficiency
A posteriori investigation	Upstream compliance, downstream insurance

Figure 3. Paradigm shift between investigation and intelligence.

Penal neo-positivism, reinforced by increasing algorithmic computing power, has the ambition to predict the future through the notions of dangerousness, of the victimization and of crimes commission. Known as a predictive policing, this movement is theorized by Ken Pease (Benslimane 2014) and applies the analytical techniques (especially quantitative) to identify probable targets for police intervention (i.e., facts, people, and locations). It allows crime prevention or the resolution of past crimes through statistical forecasts.

The willingness to produce the truth is replaced by the willingness to control a risk, thus causing a shift in the values of the police system—it is no longer necessary to do justice to the past for redemption, but it is more useful to regulate the present in order to mitigate the risk, or even to anticipate the future risks. The criminal investigation is replaced by an upstream compliance and a downstream insurance. It is no longer useful to lament the past, but it is a priority to quickly rebuild on the ashes of the past. This approach is characteristic of a society based on movement, speed, and forgetting, where the flow is more important than the stock.

Consequently, is this police posture a new utopia that seeks to have an impact on crime via new information and communication technologies (computer networks, computing power, metadata, artificial intelligence)? It renews the unfulfilled promise of positivism—are we now able to provide a solution to crime?

Before that, the law enforcement agency has settled this debate; the private sector is pragmatically embarked on this path thanks to the networked computer environment, then to big data, and now to artificial intelligence.

We observe that the representatives of the collective interest protect less efficiently the individuals, and that the representatives of particular advantage protect themselves from the collective risks in the meantime. Consequently, in order to protect their main interests, the enterprises are learning to dispense the protection of the States and to develop their own detection and remediation systems to face the cyber threats. In data-driven logic, they are performing a very sophisticated analysis of the threat and the risk assessment in order to adapt the capacities and hindrance accordingly. From a methodological point of view, based on the anticipation by the detection of weak signals and the implementation of particularly diversified solutions, the enterprises are adopting a posture closer to the matter of intelligence than investigation.

To this end, the prevention and repression of cyber threats are emblematic of this paradigm shift from investigation to intelligence.

2. From Investigation to Intelligence

2.1. In the Public Sector

The repression of cybercrime by the public actors has adapted homeostatically to its changing context. The scope of its actors, its means of detection, its investigative procedures, and its methods of remediation borrow from techniques that are fundamentally different from the traditional penal system. Without claiming to be exhaustive, it is appropriate here to give a few examples of this adaptation.

The functioning of the internet is based on a set of actors whose existence is necessary for its operation and regulation: access providers, site managers, hosts, registrars, information systems, security agencies, regulatory authorities, etc. The internet is also a tool for the protection of the public and the protection of the environment. Each one has a role and holds information that is useful for the manifestation of the truth. Some have the means to make this truth appear very quickly through mass data management tools. The government organizations are not always the most advanced in this field and must necessarily collaborate with the private sector. Indeed, the information is mainly obtained with a collective effort.

In order to overcome the low reporting of cybercrime, the law enforcement agencies are now moving from a complaints system to a reporting system (Barlatier 2020). As a result, victim complaints are no longer mandatory to the opening of an investigation. The data collected on dedicated online

platforms (PHAROS, ACYMA, PERCEVAL) improve the understanding of the phenomena and their evolution. The centralization and the analysis of these data, which are previously dispersed, help to respond appropriately. In this context, the investigation then becomes only one response to the delinquency among others.

Moreover, in the post-attack context, the criminal investigation has no longer the monopoly on the collection of intelligence under duress. While many States have authorized direct access to internet giants' data by their intelligence services (United States, China) or have restricted access controls to their network (Russia, China), France has provided a legal framework, since 2015, for the use of intelligence gathering techniques (TRR—techniques de recueil de renseignement): access to connection data, interception of communications, remote data capture, use of "black boxes" allowing real-time data collection, and the implementation of detection algorithms, etc. The use of these techniques is now subject to a legal framework. As they do not require the prior authorization of the judicial judge, which is the guardian of the individual liberties, these intelligences that gather and process procedures are on the upstream work of the criminal investigations to prevent crime by other means. This development is part of a continuum between defense, internal security, and economic security.

The criminal intelligence approach explores a wide range of remedial measures. The penal neutralization, via investigation, is one of the measures, although it is not always the most effective. We observe the same for the administrative hindrance through regulation of the internet in a deregulated system—constantly adapting and essentially international. Besides, partnership-based remediation with internet players seems more appropriate. It consists in making internet professionals or those who are carrying out their activity on the internet in a responsible way by using their interests (e.g., economic or reputational) to put an end to vulnerabilities that are exploited by offenders. Criminal risk management is affecting the companies' risk management. This partnership-based remediation is also used to warn internet users of the frauds of which they could be victims. Indeed, cybercrimes are acts that can be avoided if internet users are sufficiently informed of the precautions to be taken: dodging online scams, prevention of attacks on automated data processing systems, good practices in terms of damage to reputation. Through appropriate actions, an informed internet user can considerably reduce the risk of online victimization.

Consequently, criminal intelligence gathers the elements necessary to understand the delinquent situations, identifies weak signals that can be detected upstream, decides on the most appropriate remedial measures, and implements them effectively. In this respect, criminal intelligence is a way of translating risk theories into crime control. Cybercrime is a promising area for experimentation in this respect. However, public intervention alone is not enough and must be supported by the complementary action of private actors.

2.2. In the Private Sector

The prevention of cyber threats by private actors is based on risk anticipation and the immediacy of the threats. Within large companies, information systems security (ISS) is most often organized internally by the creation of computer security incident response teams (CSIRT) and security operation centers (SOC) designed to prevent or fix computer attacks. Their main missions are the implementation of the system protection processes, closing security gaps, analyzing data and defining detection patterns, monitoring and identifying weak signals, implementing counter-measures in case of attack on automated data processing systems, and sharing threat-related information. They protect the company from malware, ransomware, or other advanced persistent threats (APT) that can cause business interruption or data leakage, which can be highly detrimental to the company's business.

In a complementary way, the development of cyber-threat intelligence (CTI) devices gives ISS actors the means and methods to the crime control, terrorism, and cyber spying. It is no longer a question of monitoring, investigating, and repressing cyber-malware, but of taking a proactive approach to intelligence based on multi-source collection (on the clear or the dark web, of human or technical origin) helping to understand, to track the threats, and to be able to attribute the cause to the right

criminal groups or organizations. The understanding of the modus operandi and motivations help to develop countermeasures at a tactical level, to adapt the company's ISS systems at an operational level, and to enable its managers to take measure of the risks linked to digital technology at a strategic level. This logic is fundamentally intelligence-based. It places the casuistic approach and the rebuilding of the past, that are characteristics of the investigation, at the heart of this one.

Consequently, criminal intelligence provides solutions that are considered promising for mass delinquency management instead of investigation. To this end, the fight against cybercrime is, in many respects, representative of this paradigm shift in the modes of production of knowledge useful in crime control.

These skills, which are developed by the private sector, can now benefit the law enforcement agencies. It is up to them to combine their action with the CSIRTs in the framework of independent, sequenced, or joint interventions.

Key points

- Methods of social regulation and crime control are dependent on the context in which they operate.
- The reactive logic of reconstructing the truth has been imposed through investigation for two centuries. Each act of delinquency is individually analyzed within the framework of a legal and rational process.
- However, this system of knowledge production is limited facing the massive increase of delinquency—firstly, damage to property, then economic and financial delinquency, then drug trafficking, and finally cybercrime.
- These four suspicions justify the need to devise some new forms of social regulation based on anticipating them through risk, and no longer on reacting to acts. This dynamic approach multiplies diversified mass solutions to delinquency.
- This logic is already at work in the prevention and the repression of cybercrime. The latter illustrates the shift in criminal investigation towards criminal intelligence, which seems much more promising.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

Barlatier, Jerome. 2017. *Management de l'enquête et Ingénierie Judiciaire, Recherche Relative à L'évaluation des Processus D'investigation Criminelle*. Thèse de Doctorat en Criminologie. Lausanne: UNIL/École des Sciences Criminelles. [CrossRef]

Barlatier, Jerome. 2019. *L'enquête Judiciaire Est-elle une Réponse Appropriée à la Cybercriminalité?* Revue de la Gendarmerie Nationale, 4ème Trimestre. Melun: Centre de recherche de l'école des officiers de la gendarmerie nationale, pp. 159–62.

Barlatier, Jerome. 2020. *De L'enquête au Renseignement, Changement de Paradigme Pour la Victime*. Paris: AJ Penal, pp. 17–20.

Benslimane, Ismael. 2014. Étude Critique d'un Système D'analyse Prédictive Appliqué à la Criminalité: Predpol®. Available online: https://cortecs.org/wp-content/uploads/2014/10/rapport_stage_Ismael_Benslimane.pdf (accessed on 17 September 2020).

Bitner, Egon. 1970. *The Functions of the Police in Modern Society: Review of Background Factors, Current Practices ans Possible Role Model (N° 2059)*. Cambridge: Oelgeshlager, Gunn & Hain.

Bratton, William. 1998. *Turnaround*. New York: Random House.

Brodeur, Jean-Paul. 1993. La pensée postmoderne et la criminologie. *Criminologie* 26: 73–121. [CrossRef]

Dregoir, Melanie, and Klein Edouard. 2017. *L'effet Iceberg et la Cybercriminalité, Étude Service Central de Renseignement Criminel de la Gendarmerie Nationale*. Melun: centre de recherche de l'école des officiers de la gendarmerie nationale.

Foucault, M. 1972. *Théories et Institutions Pénales. Cours au Collège de France 1971–1972*. Paris: EHESS Gallimard Seuil.

Goldstein, Hermann. 1990. *Problem-Oriented Policing*. Philadelphia: Temple University Press.

Home Office. 2010. *Guidance on the Management of Police Information*, 2nd ed. London: National Police Improvement Agency. Available online: https://ict.police.uk/wp-content/uploads/2016/07/mopi-refreshed-guidance.pdf (accessed on 17 September 2020).

Jobard, Fabien, and Jacques de Maillard. 2015. *Sociologie de la Police. Politiques, Organisations, Réformes*. Paris: Armand Collin, 298p.

L'Heuillet, Helene. 2001. *Basse Politique et Haute Police, une Approche Historique et Philosophique de la Police*. Paris: Fayard.

Lipovetsky, Gilles, and Sébastien Charles. 2004. *Les Temps Hypermodernes*. Paris: Grasset, 122p.

Loveday, Barry. 2018. The Shape of Things to Come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the Police Service of England and Wales. *Policing: A Journal of Policy and Practice* 12: 398–409. [CrossRef]

Massé, Michel, Jean-Paul Jean, and Andre Giudicelli. 2009. Prologue, le droit pénal au prisme de la postmodernité, évolutions et ruptures. In *Un Droit Pénal Postmoderne?* Edited by M. Massé, J. P. Jean and A. Giudicelli. Paris: Presses Universitaires de France.

ONDRP. 2019. Rapport D'Enquête « cadre vie et sécurité », Année 2018, Observatoire National de la Délinquance et des Réponses Pénales, Service Statistique Ministériel de la Sécurité Intérieure, Décembre. Available online: https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-Cadre-de-vie-et-securite-2019 (accessed on 17 September 2020).

Peretti-Watel, Patrick. 2001. *La Société du Risqué*. Paris: La découverte, 124p.

Ratcliffe, Jerry. 2016. *Intelligence-led Policing*. Cullompton: Willan.

Reiner, Robert. 1992. Policing a postmodern society. *The Modern Law Review* 55: 761–81. [CrossRef]

Skogan, Wesley. 2004. *Community Policing: Can it Works?* Belmont: Wadsworth/Thomson Learning.

Zedner, Lucia. 2007. Pre-crime and post-criminology? *Theorical Criminology* 11: 261–81. [CrossRef]