Cyber Law Enforcement and Investigations: A Review

*Dr. Rajeev Srivastava
**Rajesh Koolwal

Abstract

Cyber Law and investigations examines law enforcement cybercrime investigations from a range of perspectives, including legal powers for investigatory measures, subject privacy safeguards, investigation challenges and good practices, interactions between law enforcement and the private sector, and law enforcement training and capacity. It demonstrates the complexities of cybercrime investigations and the need for effective legal frameworks, combined with law enforcement resources and skills in practice.

Keywords: Cyber Law, Privacy Safeguards, Law enforcement training, Cybercrime Investigation

I. Introduction

Article 1 of the United Nations Code of Conduct for Law Enforcement Officials[1] highlights that the role of law enforcement is to fulfil the duty imposed upon them by law, *'by serving the community*' and '*by protecting all persons against illegal acts*.' This duty extends to the full range of prohibitions under penal statutes.[2] As cybercrime acts become ever more prevalent, law enforcement agencies increasingly face the question of what it means to 'serve' and 'protect' in the context of a crime with global dimensions. More than half of countries reported that between 50 and 100 per cent of cybercrime acts encountered by the police involve a *transnational* element. At the same time, responding countries indicated that the majority of cybercrime acts come to the attention of the police through individual victim reports. Cybercrime thus *occurs globally*, but is *reported locally*. The report may reach a national cybercrime hotline or specialized police unit, but can also reach a municipal or rural police office more accustomed to dealing with 'conventional' burglary, robbery, theft, or homicide. In the same way as 'conventional' crime, however, both 'cyber' victims and 'cyber' perpetrators are real individuals with real geographic locations – both of which fall within a local police jurisdiction.

Local police stations may often transfer cybercrime cases to a specialized national-level law enforcement lead. However, the growing involvement of electronic evidence in *all* crime types is likely to revolutionize policing techniques, both at central *and* local level, in the coming decades. In some countries, for example, local police stations have been routinely equipped with desktop technology for extracting mobile phone data from suspects.[3] Country responses to the Study

questionnaire highlight considerable variation in the capacity of police forces to investigate cybercrime both between and within countries. As one country noted: '*The police corps of the localities differ a lot when it comes to cybercrime. Some have well organized cyber units, others barely have a few trained officers*.'

An incident-driven response to cybercrime must, however, be accompanied by medium and long-term strategic investigations that focus on disrupting cybercrime markets and bringing to justice criminal scheme architects. The prevention of *any* form of crime requires a proactive and problem-oriented approach to policing, with police working alongside other multidisciplinary partners[4] towards the overall aim of the maintenance of social order and public safety.[5] Notions of police 'community' engagement and 'public safety' require some translation in the move from the offline world to the online world. Nonetheless, country responses to the Study questionnaire suggest that this principle, as well as many other elements of police good practice in the prevention of 'conventional' crime, are equally applicable when it comes to cybercrime. These especially include the need for law enforcement agencies to work with private sector and civil society partners, and to apply 'intelligence-led' policing to pre-empt and prevent cybercrime – using problem-solving approaches based on sound information and 'horizon scanning.' As highlighted by one responding country, for example: '*attacks are becoming more and more advanced, more and more difficult to detect and in the same time the techniques quickly find their way to a broader audience*.'

II. What Do The Police Confrontation?

Many countries stated that more than 90 per cent of acts that come to the attention of the police through reports from individual and company victims. The remainder of acts were reported to be detected directly by police investigators or obtained from ISP reports. The picture of cybercrime seen by law enforcement is, being constructed from a mixture of individual investigated cases and broader criminal intelligence. The transnational nature of cybercrime exacerbates the challenge, as investigative leads arrive at overseas servers or IP-addresses, creating delays while formal or informal cooperation mechanisms are engaged. For example, '*Most of the crimes, including the unreported ones, involve transnational dimensions. Targets are mostly outside of national boundaries*.' In addition to transnational elements, significant *under*reporting of cybercrime acts in the first place can contribute to a limited picture of the underlying phenomenon. Of the 90 per cent of cybercrime acts that come to the attention of the police through victim reporting, countries estimate that the proportion of *actual* cybercrime victimization reported to the police ranges upwards from only one per cent. One survey conducted by a private sector organization suggests that 80 per cent of individual victims of core cybercrime acts do not report the crime to the police.[6] Underreporting of cybercrime acts to a number of factors, including a lack of public confidence in the capacity of police to address

cybercrime, a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. for example, stated that: '*Estimation is very difficult. Companies and banks are not interested in reporting cybercrimes due to reputational risks*.' When cases do come to the attention of the police, subsequent investigation may reveal a much wider pool of victims and offenders than initially identified at the outset of a case. Country responses also showed the need for law enforcement authorities to work closely with other stakeholders, such as the private sector – in order to increase reporting and for intelligence purposes. Overall, the comparatively low proportion of cybercrime acts reported by company victims or internet service providers, suggests that additional outreach and development of public-private partnerships may be needed, in order to strengthen reporting of cybercrime acts from these sources. Interactions between law enforcement and third party service providers during police investigations to be addressed. Responding countries did not, in general, refer to proactive investigations in written responses to the questionnaire.. The distribution of the source of identified cybercrime acts is indicative, in part, of the challenge of addressing both *strategic* and *tactical* policing objectives. Strategic policing objectives are threat-driven and relate to longer-term law enforcement goals, with a focus on the root causes and circumstances of serious crime. Tactical policing objectives are incident-driven and time-sensitive, with an emphasis on preserving evidence and following investigative leads. In the case of cybercrime, the investment in police time and resources required for responding to individual cases is substantial. In many countries, law enforcement agency capacity is fully occupied with day-to-day cases. In addition to the challenge of capacity and resources, the extent to which proactive cybercrime investigations can be undertaken by law enforcement may also be affected by underlying differences between common and civil law systems regarding prosecutorial and judicial oversight over the initial stages of an investigation,[7] as well as the extent to which intrusive investigative measures can be authorized in intelligence-based or prospective investigations. Cybercrime investigations often make use of tools, including interception of communications and electronic surveillance, which have the potential to infringe upon privacy-based rights. Countries with international human rights law commitments will need to ensure a proportionate balance between protection of privacy, and infringements for legitimate crime prevention and control purposes. Law enforcement authorities in developed countries, and also in developing countries, are engaged in medium and long-term strategic investigations. These often involve undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and P2P services. Examples include the infiltration or establishment of online 'carding' forums,[8] the forensic examination of forums used by child pornography offenders,[9] the use of law enforcement officers posing as minors online,[10] and the examination of malware command and control servers.[11] Many of these investigations involve multiple law enforcement agencies and a large range of investigative measures, including those carried out pursuant to

judicial authority, such as search or interception orders. Indeed, both strategic and tactical investigations require access to a range of investigative powers, which – in accordance with rule of law principles – must be firmly grounded in legal authority.

III. Cyber-specific And General Investigative Controls

The evidence of cybercrime acts is almost always in electronic, or digital, form. This data can be stored or transient, and can exist in the form of computer files, transmissions, logs, metadata, or network data. Obtaining such evidence requires an amalgamation of traditional and new policing techniques. Law enforcement authorities may use 'traditional' police work like interviewing victims or undercover visual surveillance of suspects, in some stages of an investigation, but require computer-specific approaches for other parts. These can include viewing, and seizing or copying, computer data from devices belonging to suspects; obtaining computer data from third parties such as internet service providers, and – where necessary – intercepting electronic communications. While some of these investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. In other countries, however, traditional procedural laws might not be capable of being interpreted to include intangible data or IP-based communications. In addition, investigative powers must be able to address challenges such as the volatile nature of electronic evidence, and use of obfuscation techniques by perpetrators – including the use of encryption, proxies, cloud computing service, 'innocent' computer systems infected with malware, and multiple routing of internet connections.[12] These aspects, in particular, present particular challenges to traditional powers. Legal frameworks for the investigation of cybercrime – whether predominantly 'general' or 'cyber-specific' laws – thus require both: (i) a clear scope of application of the power, in order to guarantee legal certainty in its use; and (ii) sufficient legal authority for actions such as ensuring preservation of computer data, and the collection of stored and real-time data. In this respect, specialized procedural frameworks offer the possibility to clearly define relevant concepts – such as 'computer data' in the first place, as well as data 'at rest' and data 'in transit.'[13] They also allow differentiation between types of data, such as 'subscriber' data (such as name and address), 'traffic' data (data indicating the origin, destination, route, time, date, size, duration, or type of a communication made by means of a computer system), and 'content' data (the actual content of a communication).[14] The existence of either general or cyber-specific legal powers for 10 different actions relevant to law enforcement investigations into cybercrime are: (i) law enforcement search for computer hardware or data; (ii) seizure of computer hardware or data; (iii) order to a person for supply to law enforcement of subscriber information; (iv) order to a person for supply of stored traffic data; (v) order to a person for supply for stored content data; (vi) real time collection of traffic data; (vii) real-time collection of content data; (viii) order to a person to

preserve and maintain the integrity of computer data under their control for a specified period of time ('expedited preservation' of data); (ix) use of remote computer forensics tools; and (x) direct law enforcement access to extraterritorial computer data ('trans-border' access to computer data). The Majority of countries rely on *general* legal powers for the investigation of cybercrime. This is the case across a range of investigative actions, including search, seizure, orders for data addressed to third parties, real-time collection of data, and orders for preservation of data. For more intrusive, complex, investigative measures such as remote computer forensics, almost half of responding countries indicated that such measures were not authorized by law. Some countries rely that no legal power existed for real-time collection of computer data, or for ordering expedited preservation of computer data. Even for basic search and seizure of computer hardware or data, and few countries rely that no legal power existed.

IV. Preservation Of Computer Data

Computer data is typically stored only for the amount of time for which it is needed for processing. In the case, for example, of 'chat' or VOIP content that passes through a service provider's service, this might only be for the amount of time needed for operational purposes, such as the identification of system faults, or customer billing. This could range from a few seconds, to hours, or a few days, or weeks. In addition to the pragmatic cost implications of data storage, many countries also have data protection frameworks that specify that data must not be retained for periods longer than that required by the purposes for which the data are processed.[15] Due legal process requirements, or – in transnational cases – international cooperation requests, may easily take a longer time than the lifespan of the data, before the relevant search warrant or order for supply of stored data can be obtained.[16] As a result, seven international and regional cybercrime instruments contain provisions aimed at establishing mechanisms for preventing the deletion of computer data important to cybercrime investigations.[17] Such actions may be given effect to by an order to a person in control of computer data to preserve and maintain the integrity of the data for a specified period of time, or by expedited procedures for otherwise securing the data, such as through a search and seizure warrant. Key features of typical 'expedited' preservation provisions may include application of a more limited set of conditions and safeguards than for disclosure of the data, due to an arguably less prejudicial nature of the preservation measure (before the point of any disclosure). In this respect, however, it should be noted that international human rights mechanisms have held that mere storage of information about an individual amount to an interference with rights to private life. Exercise of preservation orders therefore still requires an assessment of the proportionality of the measure – in particular where compliance with the order would require specific data to be held for longer than the time period envisaged by data protection legislation. Nonetheless, preservation of data represents an important measure for maintaining vital evidence prior to a full order for disclosure – in particular

in the context of transnational investigations. Indeed, the separation of the two obligations, 'preservation' and 'disclosure' is a key element of the measure.[18] At the national level – perhaps due to the influence of international and regional cybercrime instruments – expedited preservation of data is the measure in respect of which the highest proportion of countries report a cyber-specific power. Nonetheless, country responses also indicated that general provisions could cover the measure in various ways. For example, that provisions on search and seizure were interpreted as providing for expedited preservation as well as that computer data can be preserved according to its legislation by means of computer seizure. In addition, however, some countries indicated that national law did not include a power to ensure expedited preservation of data. The absence of legal authority for such a fundamental investigative tool presents a significant challenge – not only for those particular countries, but also for any other country wishing to seek investigative assistance.

V. Conclusion

It is clear that local police agencies are still in the early stages of developing comprehensive strategies for responding to and preventing cybercrime. Additional work needs to be done to ensure that every police officer will know how to respond to a cyber-crime call; detectives will understand the avenues that are available for investigating these crimes; and local, state, and federal authorities will have an effective system for sharing information, connecting cases committed by the same offenders, and coordinating investigations. These steps include:

- **Participating in task forces.** Task forces use the resources of local, state, and federal agencies to investigate cases that would be too large or complex for one agency to handle alone. Electronic Crime Task Forces (ECTFs), and Regional Computer Forensics Labs (RCFLs), created by the FBI, provide federal assistance on a regional basis.
- **Working with private corporations.** In many cases, private corporations have more experience with cybercrime investigations than local police agencies. Corporate officials often have a great deal of respect for their local police officials and are glad to build these partnerships.
- **Working with regional universities.** A number of police agencies have formed partnerships with computer science departments at local universities. These partnerships not only provide expertise to the police, but also serve as a recruiting tool for students who have an interest in cybercrime and policing.
- **Identifying, recruiting, and training talented personnel.** Police departments need employees who are capable of handling cybercrime issues. Some police departments are undertaking a variety of strategies for identifying and recruiting potential employees with knowledge of information technologies, and identifying current police employees who have an interest in cyber issues and can be trained to play an important role in the department's cybercrime prevention and investigation efforts.

- **Educating the community.** Many cybercrimes are preventable by taking appropriate security measures while using electronic devices. To protect community members from becoming victims of cybercrime, police departments should have education programs to teach people about common cyber-threats and the basics about how they can stay safe online.

Research Guide,
Mahatama Jyoti Rao Phoole University,
& Principal, LBS P.G. College,
Jaipur (Rajasthan-302004), India
****Research Scholar,***
Mahatama Jyoti Rao Phoole University,
Jaipur (Rajasthan-302004), India

References

Journal References

1. *Code of Conduct for Law Enforcement Officials, Art.1. Annex to General Assembly Resolution 34/169, 17 December 1979*
2. *Ibid., Commentary to Art. 1, at (d).*
3. *http://www.bbc.co.uk/news/technology-18102793*
4. *UNODC. 2010. Handbook on the Crime Prevention Guidelines: Making them work.*
5. *Bowling, B., and Foster, J., 2002. Policing and the Police. In: Maguire, M., Morgan, R., Reiner, R. (eds.). The Oxford Handbook of Criminology. 3rd edn. Oxford: Oxford University Press.*
6. *Symantec. 2012. Norton Cybercrime Report 2012.*
7. *INPROL. 2012. Practitioner's Guide: Common Law and Civil Law Traditions.*
8. *http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 and 2012/manhattan-u.s.-attorney -and-fbi-assistant -director-in-charge- announce-24-arrests-in-eight-countries-as-part-ofinternational- cyber-crime-takedown*
9. *https://www.europol.europa.eu/sites/default/files/publications/2csefactsheet2012_0.pdf*
10. *http://cdrc.jhpolice.gov.in/cyber-crime/*
11. *http: // www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin, %20Nikita% 20 Complaint.pdf*
12. *Feigenbaum et al., 2007. A Model of Onion Routing with Provable Anonymity. Financial Cryptography and Data Security Lecture Notes in Computer Science, 4886:57-71; and Schwerha, J.J., 2010. Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers," Council of Europe Discussion paper, pp.9-10; Walden, I., 2013. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. Privacy and Security for Cloud Computing. Computer Communications and Networks 2013, pp.45-71.*

13. *Walden, I., 2003. Addressing the Data Problem. Information Security Technical Report, 8(2); Nieman, A., 2009. Cyberforensics: Bridging the Law/Technology Divide. JILT, 2009(1).*
14. *Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In: Delmas- Marty, M., Pieth, M., Sieber, U. (eds.). Les chemins de l'HarmonisationPénale/Harmonising Criminal Law.*
15. *Section 8.3 Cybercrime prevention, the private sector and academia, Cybercrime prevention by internet service and hosting providers.*
16. *James Tetteh, A.-N., Williams, P., 2008. Digital forensics and the legal system: A dilemma of our times. Available at:http://ro.ecu.edu.au/adf/41/*
17. *Draft African Union Convention, Art. 3-53; COMESA Draft Model Bill, Arts. 33-35; Commonwealth Model Law, Art.17; Council of Europe Cybercrime Convention, Art. 16; ECOWAS Draft Directive, Art. 33; ITU/ CARICOM/ CTU Model Legislative Texts, Art.23; League of Arab States Convention, Art. 23.*
18. *See Brown, I., 2010. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology, 19(2):107.*