Cybercrime: Policing and Prosecution

Research Handbook on Transnational Crime

Professor Petter Gottschalk, BI Norwegian Business School, Oslo, Norway

INTRODUCTION

Cybercrime policing and prosecution have both similarities and differences when compared to traditional crime such as human trafficking and drug smuggling. Traditional crime generally concerns offences against the person or property offences. Cybercrime is characterized by being technologically advanced, it can occur almost instantaneously, and it is extremely difficult to detect and investigate. However, cybercrime can also be easy to track, when digital detectives can follow electronic leads.

While a technological crime scene may be easy to track, the criminal actors are more difficult to find and prosecute. The problem of offender identification is a result of the relative anonymity afforded by the Internet as well as the transcendence of geographical and physical limitations in cyberspace. In addition, decentralised peer-to-peer networks may prevent material from being tracked to a specific location, and sophisticated encryption lets criminals keep online chats private from those policing the web.

Transnational cybercrime encompasses illegal activities carried out across national borders [1] using information technology. Criminals are able to take advantage of a virtually limitless pool of potential victims. This is the case, for example, in online grooming where paedophile offenders find child victims in jurisdictions across borders[2]. Similarly, transnational music piracy is committed through a multitude of modus operandi and in various jurisdictions[3]. In addition, financial crime in terms of, for example, electronic money laundering is frequently transnational between banking sectors with different legislations and secrecy practices[4].

This chapter addresses the issues of policing and prosecuting cybercrime. Policing is discussed in terms of knowledge management, where a key knowledge category in law enforcement is digital competence. Prosecution is discussed in terms of knowledge rivalry, where knowledge rivalry occurs between prosecutors and defence lawyers in court.

THE CASE OF ONLINE GROOMING

[1] Gottschalk, P. and Markovic, V. (2016). Transnational criminal organizations (TCOs): The Case of Combating Criminal Biker Gangs, International Journal of Criminal Justice Sciences, 1, pages 1-12.

[2] Davidson, J. and Gottschalk, P. (2015). The Context of Online Abuse: Policy and Legislation, in: Webster, S., Davidson, J. and Bifulco, A. (editors), Online Offending Behaviour and Child Victimisation, Palgrave Macmillan, UK: London, pages 1-20.

[3] Higgins, G.E., Wolfe, S.E. and Marcum, C.D. (2008). Music Piracy and Neutralization: A Preliminary Trajectory Analysis from Short-Term Longitudinal Data, International Journal of Cyber Criminology, 2(2), 324-336.

[4] Filstad, C. and Gottschalk, P. (2012). Characteristics of White-Collar Criminals: A Norwegian Study, Journal of Money Laundering Control, 15 (2), 175-187.

The sexual abuse of young people via the Internet is an international problem, a crime without geographical boundaries. Adults use the Internet to befriend and establish an emotional connection with a child, in order to entice them into meeting. As more young people use the Internet to socially network with friends, the potential for contact with sexual offenders will increase. There is, however, limited information available about the behaviours of Internet sexual offenders to inform effective risk management strategies for policy makers, law enforcement agencies, parents, and young people. In response to this, the European Commission Safer Internet Plus Program commissioned a consortium of leading experts from the UK and across Europe to develop an understanding of the different ways in which sexual offenders approach, communicate and 'groom' young people online. Davidson and Gottschalk[5] report findings from the European project based on interviews of both experts and offenders in the UK, Belgium, Italy, and Norway. The below comments are findings from the report.

There is increasing evidence that adults use the Internet more and more to access children and young people for the purposes of sexual abuse. Internet sex offender behaviour includes the construction of sites to be used for the exchange of information, experiences, and indecent images of children; the organisation of criminal activities that seek to use children for prostitution purposes and that produce indecent images of children at a professional level, and the organisation of criminal activities that promote sexual tourism. The definition of an online groomer is someone who has initiated online contact with a child with the intention of establishing a sexual relationship involving cyber-sex or sex with physical contact. Child grooming is a process that commences with sex offenders choosing a target area that is likely to attract children. In the physical world, this could be venues visited by children such as schools, shopping malls or playgrounds. A process of grooming commences when offenders take a particular interest in the child and make them feel special with the intention of forming a bond as a precursor of abuse. The Internet has greatly facilitated this process in the virtual world in terms of geographic location, speed of contact, range and number of contacts.

Groomers will often offer incentives such as money, gifts, concert tickets, modelling contracts, day trips, phones and games as part of the grooming process or to encourage young people to produce and send personal images. Internet sexual offenders are currently defined as falling into two principal categories, which are not mutually exclusive: those who use the Internet to target and groom children for the purposes of sexual abuse; and those who produce and/or download indecent illegal images of children from the Internet and distribute them.

Recent advances in computer technology have been aiding sex offenders, stalkers, child pornographers, child traffickers, and others with the intent of exploiting children. While such offences occurred prior to the Internet, the advent of the new technology two decades ago has allowed for easier and faster distribution of pornographic materials and communication across national and international boundaries. The dynamics of this opportunism is the subject of ongoing discussion. In his research with a sample of 300 child pornography offenders, Hernandez comments that it is through the exploration of sexual themes and seeking out adult pornography on the Internet that their previous deviant sexual interests are reawakened.

The Internet provides the opportunity to join a virtual community where people with similar interests can communicate and find useful information. 'Myspace' and other similar social networking sites encompass thriving 'communities' where young people engage in countless hours of photo sharing. In addition to Myspace, other social networking and blogging sites such as Friendster.com, Facebook.com and MyYearbook.com allow users to post pictures, videos and blogs and send emails and instant messages. Myspace and Facebook differ in

[5] Davidson and Gottschalk (n 2)

security aspects in that Myspace is open to anyone, and has loose age restrictions, while Facebook users are encouraged and often required to register using their real name. The anonymity, availability of extremely sensitive personal information and ease of contacting people, make social networking sites a useful tool for online child sex offenders in general, but specifically for online groomers. Usage by young people develops, whereby if young people want to get to know each other better, then they may move into more private arenas such as MSN. This intensifies the communication, and if the relationship is developed further, then they might show and invade a private space of web cameras.

While many of these sites have age restrictions, it is possible for offenders to misrepresent their age. In addition, in order to hide their IP addresses and locations, offenders can piggyback on insecure Wi-Fi connections or use proxy servers. Decentralised peer-to-peer networks prevent material from being tracked to a specific server, and encryption lets them keep online chats private from those policing the Internet.

Therefore, technologies around social networking sites allow relatively easy access to children by online groomers, with children having frequent and open access to such sites at younger ages. Once in contact with a child, the online groomers can use various incentives to encourage the child's participation, towards the goal of sexual contact.

OTHER CYBERCRIME EXAMPLES

Herley[6] distinguishes between financially and non-financially motived cybercrime. Online transnational grooming is an example of non-financially motivated cybercrime. When money is the goal, it seems reasonable to assume that an offender is sufficiently motived when the expected gain from an attack exceeds the cost. This is in line with rational choice theory, which is turn is integrated into convenience theory as an explanation for financial crime.

Convenience theory suggests that an offender with a financial motive, a technology opportunity, and a deviant behaviour will commit financial crime[7]. The technology opportunity includes access to the Internet and skills to manipulate computer programs and digital information. The technology opportunity also includes the vast array of potential targets for attack. A financially motivated attacker will decide who and what to attack, attack successfully, and then monetize access. The attack can be against a computer system or by means of a computer system.

An example of the latter is transnational CEO fraud, which is an attack by means of email. CEO power and influence can be illustrated by what is labelled CEO fraud in law enforcement. CEO fraud is not fraud by CEOs. Rather, CEO fraud is fraud committed by someone claiming to be the CEO. If someone claims to be the CEO, most people in the organization will do what they are told. As long as they believe that the message stems from the real CEO, they are completely obedient and do as they are told by the fake CEO. The U.S. Federal Bureau of Investigation (FBI) warned in 2016 about a dramatic increase in CEO fraud, e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams cost organizations in the United States more than one billion dollars per year. Organizations that

[6] Herley, C. (2014). Security, Cybercrime, and Scale, Communications of the ACM, 57 (9), 64-71.
[7] Gottschalk, P. (2017a). Convenience in White-Collar Crime: Introducing a Core Concept, Deviant Behavior, 38 (5), 605-619.

are victimized by CEO fraud can be characterized by a combination of CEO power and obedience culture[8].

POLICING CYBERCRIME

Policing transnational cybercrime is a knowledge-intensive challenge because of the innovative aspect of many kinds of computer crime. Cyberspace presents a challenging new frontier for police science, law enforcement, and policing. Virtual reality and computer-mediated communications challenge the traditional discourse of police work, introducing new forms of deviance, crime, and social control. Criminal justice response to cybercrime includes cybercrime policing unites, which can be found in most developed countries today.

Most cybercrime policing units are involved in intelligence gathering, sharing, and transnational exchange. An example is the central criminal agency in Norway that is extensively involved in information exchange bilaterally as well as through Europol, Interpol, and the United Nations. Traditionally, intelligence was understood to mean information from criminals about criminal activity by a covert source. Today, intelligence gathering is intended to be a systematic approach to collecting information with the purpose, for example, of tracking and predicting crime to improve law enforcement. Intelligence analysts investigate who is committing crime, how, when, where and why. They then provide recommendations on how to stop or curb the commission of offenses. As part of this, analysts produce profiles of crime problems and individual targets, and produce both strategic (overall, long-term) and tactical (specific, short-term) assessments within the confines set by the policing unit.

The aim of an intelligence strategy is to continue to develop intelligence-led policing in all parts of an organisation, a nation or in all regions in the world. An intelligence strategy provides a framework for a structured problem solving and partnership enhanced approach, based around a common model[9]. For example, the national intelligence model in the UK is a structured approach to improve intelligence-led policing both in real spaces and in virtual spaces. Intelligence-led policing inspires objective decision-making that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement that target prolific and serious offenders.

While intelligence is concerned with the greater picture of cybercrime, investigations are concerned with specific occurrences of cybercrime. Criminal investigations are a goal-oriented process reconstructing the past. They are a method of creating an account of what has happened, how it happened, why it happened, and who did what to make it happen or let it happen. Criminal investigations try to reconstruct past events and sequences of events through the collection of information and evidence[10]. An investigation is designed to answer questions such as when crime, where crime, what crime, how crime, who committed crime, and why crime was committed, as such questions relate to negative events in the past. To reconstruct the past successfully in a professional manner, there is a need for knowledge management.

Criminal investigations are based on a foundation of information gathering over time. Cybercrime investigators need to have the knowledge and training necessary to handle complex investigations. They need to have the skills necessary to reach intended objectives.

---

[8] Gottschalk, P. (2017b). CEOs and White-Collar Crime: A Convenience Perspective, Palgrave Macmillan, UK: London.

[9] Bell, P., Dean, G. and Gottschalk, P. (2010). Information Management in Law Enforcement: The Case of Police Intelligence Strategy Implementation, International Journal of Information Management, 30, 343-349.

[10] Osterburg, J.W. and Ward, R.H. (2014). Criminal Investigation – A Method for Reconstructing the Past, 7th Edition, Anderson Publishing, MA: Waltham.

Knowledge as a combination of information, interpretation, reflection and context can be defined in terms of its level or depth[11]:

A. Basic knowledge is knowledge of what has happened, it is the know-what of an offence.

B. Advanced knowledge is knowledge of how it happened; it is the know-how of a negative event. It is knowledge of modus operandi in cybercrime.

C. Innovative knowledge is knowledge of cause-and-effects in terms of causality, it is the know-why of a negative event.

According to the knowledge-based view, knowledge is a scarce resource, and the ability to manage it determines an organisation's effectiveness. Knowledge management can be defined as a systematic, organisationally specified process to acquire, organise, and communicate individual knowledge so that others may make use of it. Knowledge management is concerned with knowledge sharing and knowledge creation in organizations. Knowledge management activities include creation, acquisition, identification, storage, sharing and application of knowledge. Knowledge sharing is defined as the exchange between two or more parties of potentially valuable knowledge.

Offender profiling is an example of a knowledge task in cybercrime investigations. It is a task of predicting and profiling characteristics of unknown criminal suspects or offenders[12]. Criminal profiling is based on two assumptions. The first is behavioural consistency, which implies that an offender will show similar behaviours across offences. The second is the homology assumption, which states that if two perpetrators exhibit similar criminal behaviour, they will also possess similar characteristics.

Investigative decision making is another example of a knowledge task in cybercrime investigations. Investigative decision making takes the form of strategic decisions in terms of resourcing through to more tactical issues such as decisions to conduct searches, tasking informants, classifying documents and following digital leads. Alys et al.[13] argue that improvements to decision making have been hindered by perspectives of investigation as a craft, rather than as a science, such that digital leads are identified by expert intuition and thereby promoting perceptions that investigations are relatively simple rather than a complex activity that draws upon a broad range of knowledge.

A third example of at knowledge challenge in cybercrime investigations is reconstruction of the past. Osterburg and Ward[14] describe elements to reconstructing the past:

- Inductive reasoning: The process of reasoning beginning with specific information to form a general conclusion.
- Deduction: The process of reasoning that begins with a generalisation and moves to a particular or specific conclusion.
- Classification: The systematic arrangement of objects into categories that have one or more traits in common.

---

[11] Glomseth, R., Gottschalk, P. and Hole, A.S. (2011). Professional Values in Knowledge Organizations: The Case of Police Districts, International Journal of Police Science and Management, 13 (1), 87-102.

[12] Gottschalk, P. (2015). Private Investigations of White-Collar Crime Suspicions: A Qualitative Study of the Blame Game Hypothesis, Journal of Investigative Psychology and Offender Profiling, 12, 231-246.

[13] Alys, L., Massey, K. and Tong, S. (2013). Investigative Decision Making: Missing People and Sexual Offences, Crossroads to an Uncertain Future, Journal of Investigative Psychology and Offender Profiling, 10 (2), 140-154.

[14] Osterburg and Ward (n 10) page 319.

- Synthesis: The combining of separate parts or elements that lead toward a conclusion.
- Analysis: Examines all information available in an effort to separate the data into relevant parts for further study.
- Hypothesis: Forms the basis for an examination of information to form an assertion or tentative guess.
- Theory: A scheme of thought with assumptions chosen to fit empirical observations.

A cybercrime investigation aims to produce knowledge as to how and why the crime was committed and who was responsible for it. In the case of online grooming, paedophiles may be in contact both with potential victims and with other offenders for possible exchange of material and information. Identifying networks of offenders is often the aim of an investigation. Sources of information in such police work include victims, electronic leads and whistle-blowers.

Police investigators face the challenge of determining the authenticity of messages by using their judgment, intuition and deductive reasoning. A cybercrime investigation can be seen as composed of a number of discrete yet linked inquiry actions, including active undercover participation, which are directed towards the production of information about how and why crime occurred. Police investigators are concerned with the gathering of evidence leading to the arrest of offenders, as well as the collection and presentation of evidence and testimony for the purpose of obtaining a conviction. Securing the scene, preserving evidence, and interviewing possible victims and witnesses are at the core of police investigations[15].

Technical resources are needed in cybercrime investigations. Based on the extensive and complex nature of technology often applied in cybercrime, Hunton[16] argues that digital evidence cannot simply be recovered and examined without the use of adequate skills, tools and equipment:

> It is essential to any cyber related investigation that the most appropriate tools are selected and used by technical investigators who are not only competently skilled in the use of such tools but also have sufficient technical and investigative knowledge to undertake a wide range of digital examinations.

INFORMATION TECHNOLOGY

Information technology is vital to cybercrime investigations. First, information is found in computer systems regarding suspicious transactions and other deviant activities. Second, the examination puzzle is solved by using computers to register, store and analyse information as it is accumulated in the investigation process. In this section, information technology for cybercrime investigations is described in terms of a stages-of-growth model. A stage model identifies stages that are (1) sequential in nature, (2) occur as a hierarchical progression that is not easily reversed, and (3) involve a broad range of organisational activities and structures.

[15] Holt, T.J. and Bossler, A.M. (2012). Predictors of Patrol Officer Interest in Cybercrime Training and Investigation in Selected United States Police Departments, Cyberpsychology, Behavior, and Social Networking, 15 (9), 464-472.

[16] Hunton, P. (2011). The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation, Computer Law & Security Review, 27, 61-67, page 65.

Here, a model consisting of four stages is presented: investigator-to-technology systems, investigator-to-investigator systems, investigator-to-information systems, and investigator-to-application systems as illustrated in Figure 1[17]:

1. *Investigator-to-Technology Stage*: Tools for knowledge workers as end users are made available. End-user development refers to activities and tools that allow end-users – people who are not professional software developers – to adapt computer programmes to their needs. Personal end-user tools enable knowledge workers to use their own personal specialized tools to perform tasks anytime and anywhere.

   Most knowledge workers rely on office systems, such as word processors, voice mail, e-mail and presentation tools, which are designed to increase worker productivity. Some knowledge workers require highly specialised knowledge work systems with powerful graphics, analytical tools, and document management capabilities.

   Stage 1 can be labelled *end-user-tools* or *people-to-technology* as information technology provide knowledge workers with tools that improve personal efficiency.

2. *Investigator-to-Investigator Stage*: Information about who knows what is made available to all people involved in the investigation and to target outside transnational partners. A typical example is Schengen Information System (SIS). Search engines should normally facilitate work with a thesaurus, since the terminology in which expertise is sought may not always match the terms (and hence search words) the expert uses to classify that expertise. The aim is to record and disclose who in the organisation knows what by building knowledge directories. Often called yellow pages, the principal idea is to make sure knowledgeable people in the organisation are accessible to others for advice, consultation, or knowledge exchange. Knowledge-oriented directories are not so much repositories of knowledge-based information as gateways to knowledge, and the knowledge is as likely to be tacit as explicit.

   Social media-enabled electronic networks of practice can stimulate knowledge exchange between knowledge seekers and contributors. Building on the concept of electronic networks of practice, enterprise social media are expected to foster interpersonal knowledge exchange among private investigators as knowledge workers as well as among investigators and their sources of information[18].

   Beck et al.[19] distinguish between two kinds of network-based personalisation approaches:

   > On the one hand, there are communities of practice, which are tightly interlinked groups of people who know one another, communicate face to face, and coordinate among themselves. On the other hand, there are networks of practice, which consist of larger, more loosely interlinked, geographically distributed groups of people engaged in shared frames and practices who do not necessarily know one another or meet in person.

3. *Investigator-to-Information Stage*: Information from knowledge workers is stored and made available to everyone in the agency and to designated external partners. Data

[17] Gottschalk, P. and Dean, G. (2010). Stages of Knowledge Management Systems in Policing Financial Crime, International Journal of Law, Crime and Justice, 38 (3), 94-108.

[18] Beck, R., Pahlke, I. and Seebach, C. (2014). Knowledge Exchange and Symbolic Action in Social Media-Enabled Electronic Networks of Practice: A Multilevel Perspective on Knowledge Seekers and Contributors, MIS Quarterly, 38 (4), 1245-1270.

[19] Beck, Pahlke and Seebach (n 18), page 1247.

mining techniques can be applied here to find relevant information and combine information in data warehouses.

The system should let users incrementally direct their search towards relevant, though not initially obvious, information. This is called information discovery for exploratory search. It addresses the vocabulary mismatch problem by giving users potential intents to explore, visualising them as directions in the information space around the user's present position, and allowing interaction to improve predictions of the user's search intents[20].

At Stage 3, investigators apply the codification strategy in knowledge management. The codification strategy is both an alternative to as well as an extension of the personalization strategy at stage 2. While network-based approaches focus on systems to foster social connections between people, repository-based approaches rely on the storage of information from knowledge workers in databases, such as searchable document repositories and mechanisms for acquiring, controlling, and publishing information in knowledge work[21]. Systems at stage 2 focus on social connections among people such that users gain access to the resources of colleagues in their practice-related social networks, while systems at stage 3 assume that social connections have been established and can be protected from abuse by enabling access to electronic information that can reduce the frequency of personal requests from colleagues.

4. *Investigator-to-Application Stage*: Information systems solving knowledge problems are made available to knowledge workers and solution seekers. Artificial intelligence is applied in these systems. For example, neural networks are statistically oriented tools that excel at the application of data to classify cases into categories. Another example is expert systems that can enable the knowledge of one or a few experts to be used by a much broader group of workers. Investigator-to-application systems will only be successful if they are built on a thorough understanding of procedures in private investigations.

   Artificial intelligence (AI) is an area of computer science that endeavours to build machines exhibiting human-like cognitive capabilities. Most modern AI systems are founded on the realisation that intelligence is tightly intertwined with knowledge. Knowledge is associated with the symbols we manipulate. The exact moment when computers get better than people at certain human tasks is debatable[22].

   Case-based reasoning systems are a different way to represent knowledge through explicit historical cases. Private investigators are looking for similar cases to learn how these were handled in the past, making case-based reasoning systems an attractive application in private inquiries into suspicions of cybercrime.

Developing, acquiring, implementing and using information systems at these four levels require effective collaboration between cybercrime investigators and technology experts in professional policing locally and globally. Information systems projects tend to be complex and require the intensive coordination of different levels of expertise, resources and work efforts. Social capital is needed for the police force to be successful. Social capital can be defined as an integrated concept of actual or potential resources gained by an individual or a

[20] Ruotsalo, T., Jacucci, G., Myllmäki, P. and Kaski, S. (2015). Interactive Intent Modeling: Information Discovery Beyond Search, Communications of ACM, 58 (1), 86-92.
[21] Beck, Pahlke and Seebach (n 18).
[22] Kirkland, R. (2014). Artificial Intelligence meets the C-Suite, McKinsey Quarterly, 3, 66-75.

group from a social system or network. Social capital theory argues that the more social capital a project team possesses the more effective systems development will become[23].

[23] Ghosh, B. and Scott, J.E. (2009). Relational Alignment in Offshore IS Outsourcing, MIS Quarterly Executive, 8, 19-29.

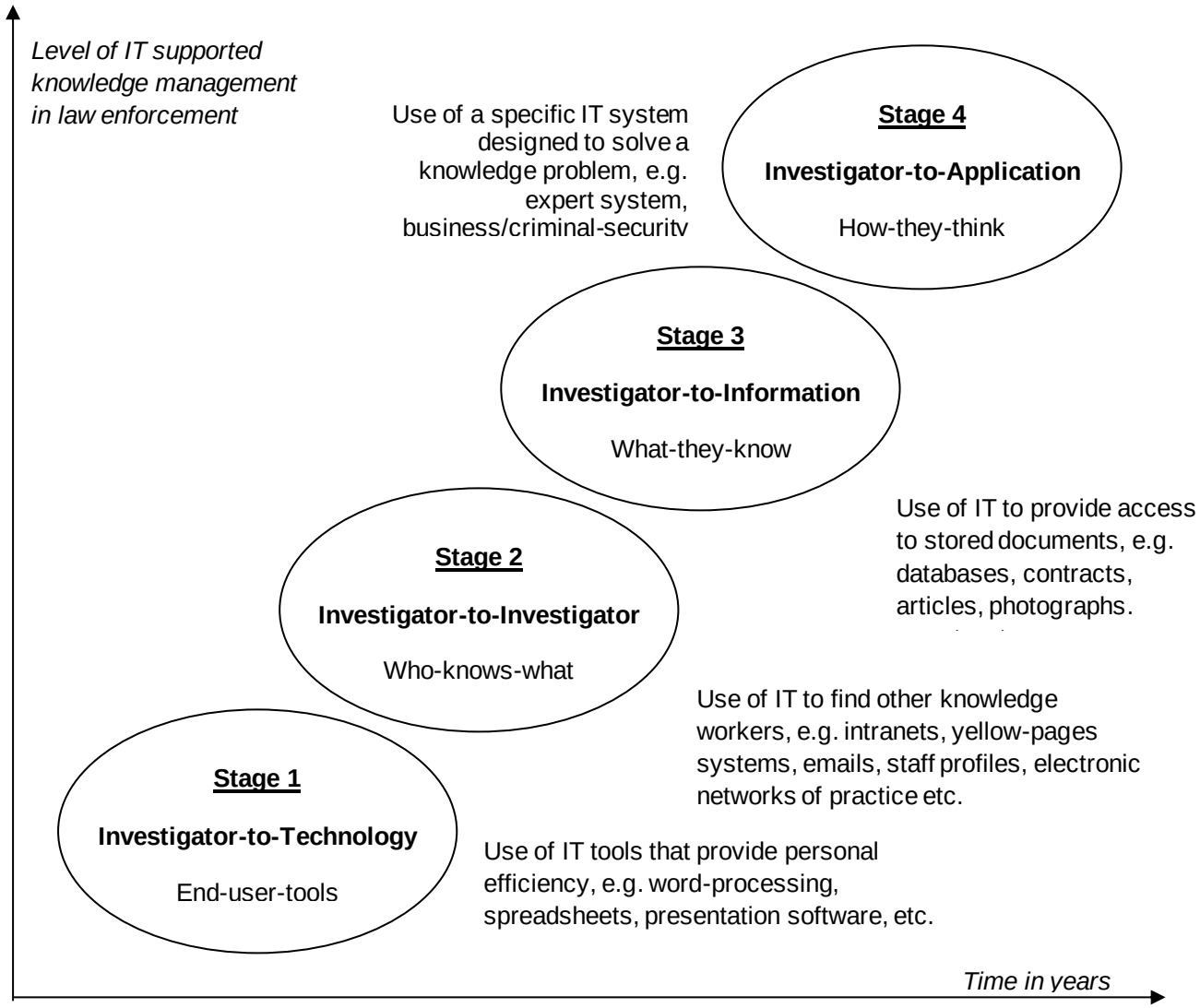

Figure 1 The knowledge management systems stage model for investigations

PROSECUTING CYBERCRIME

Cybercrime is an international problem. Serious criminal activities nearly always cross borders, often with the perpetrators operating from relatively safe territories beyond the easy reach of law enforcement agencies of the countries in which the victims reside. Mansfield-Devine[24] suggests that collaboration between governments, intelligence agencies and law enforcement officers is critical to prosecuting cybercrime, and that new organisations should be created to enable this. States should be obliged to make prosecution of transnational crime a priority. Ideally, the prosecution of crime should provide sufficient deterrence to help prevent additional violations[25].

[24] Mansfield-Devine, S. (2013). Resetting the Clock on International Co-Operation, Network Security, December, 12-16.

[25] Ortner, D. (2015). Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime, Brigham Young University Law Review, 1, 177-217.

In terms of sentencing cybercriminals both location of offender and victim influence severity and accessibility of punishment. For example, when a paedophile in Europe has abused a child in Asia on the Internet, both evidence and witness statement can be a challenge for the prosecution. This seems to make proving the crime more difficult, but probably does not affect the severity of punishment.

The prosecutor is the chief legal representative of the prosecution presenting the case in a criminal trial against an individual accused of breaking the law (Gottschalk, 2014). There are at least four persons present in court: the cybercrime defendant, the defines lawyer, the public prosecutor, and the trial judge. A trial in court is law in action, where knowledge and discretionary decision making by legal actors are central components. Prosecutors are normally granted authority to attain broad legislative goals. The process of rule into action cannot be accomplished unless legal actors interpret and make choices. In this perspective, prosecutors are powerful actors in criminal justice.

However, cybercrime can also be perceived as a prosecutorial problem. For example, there is a challenge in the application of traditional legislation to digital arenas of crime. The traditional goal of criminal law is mainly to convict individuals who commit street crime. A question of importance is whether prosecutors, like judges, pursue different goals when confronted with cybercriminals as opposed to traditional criminals. Prosecutors may pursue different punishment objectives depending on the type of offense and the type of offender. For example, their focus may be more or less on the impact of punishment on the offender and more or less on the preventive impact of punishment on the community as a whole.

From a legal perspective, a court situation is characterised by efforts to conclude whether the charged persons and company are guilty or not guilty. From a knowledge perspective, this situation is characterised by a competition as illustrated in Figure 2. Depending on the relative knowledge levels of prosecution and defence, a knowledge rivalry with three alternative situations might exist as illustrated in the figure:

1. Defence lawyers are experts, while prosecutors are not experts in areas such as online grooming, financial transactions, and music piracy. Defence lawyers have innovative knowledge (know-why), while prosecutors have core knowledge (know-what).
2. Prosecutors are experts, while defence lawyers are not experts in laws and regulations. Defence lawyers have core knowledge (know-what), while prosecutors have innovative knowledge (know-why).
3. Both parties are at about the same knowledge level, leading to a real knowledge competition in court between the defence lawyers and prosecutors.

Prosecution of cybercrime involves several special considerations as discussed by Jarrett and Bailie[26]: jurisdiction, venue, statute of limitations, and juveniles. In terms of jurisdiction, several courts in the United States have indicated a willingness to assume that a crime took place in or affecting interstate business as long as there is evidence that the defendant used the internet in connection with the offence. For example, a court rejected the argument that a wire fraud conviction required evidence that certain emails actually crossed national borders. A connection to the Internet will satisfy the requirement of jurisdiction.

[26] Jarrett, H.M. and Bailie, M.W. (2015). Prosecuting computer crimes, Office of Legal Education, Executive Office for United States Attorney, downloaded November 5, 2016, https://www.justice.gov/sites/default

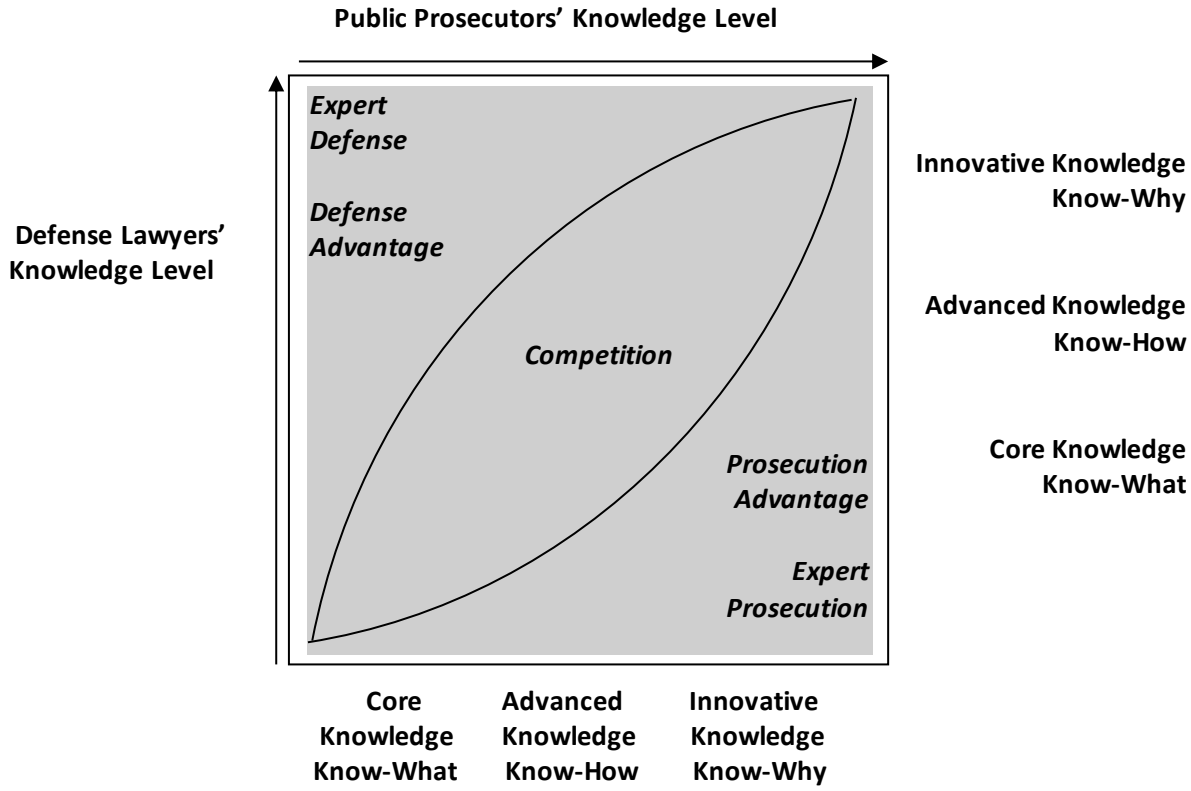

Figure 2 Knowledge rivalry between prosecution and defence in court

In terms of venue, most countries mandate that the defendant's trial location is in the nation where the crime was committed. Applying the principle of venue to network crime is not always a straightforward endeavour. In today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space. In some cases, venue might lie in the country where the effects of the crime are felt[27].

In terms of statute of limitations, it is not obvious when it is too late to prosecute a cybercrime case. For cases involving evidence located in a foreign country, prosecutors in some nations can request that the court suspend the statute of limitations[28].

In terms of juveniles, many computer hackers and other offenders may be teenagers when they commit their offences. A juvenile trial is not the same as a criminal prosecution in most countries. There is an issue to be determined whether the minor is a juvenile delinquent as a matter of status, not whether he or she is guilty of committing a crime[29].

Eurojust[30] argues that judicial cooperation is essential to ensure timely preservation of electronic evidence, which ensures its admissibility in judicial proceedings. International judicial cooperation may be hampered by significant differences in domestic legal frameworks.

[27] Jarrett and Bailie (n 26).
[28] Jarrett and Bailie (n 26).
[29] Jarrett and Bailie (n 26).
[30] Eurojust (2015). Annual Report 2015, downloaded November 5, 2016, http://www.eurojust.europa.eu/dolibary/corporate/.

CONCLUSION

As illustrated in this chapter, there are indeed challenges in policing and prosecuting transnational cybercrime. There are knowledge challenges among detectives and prosecutors, there are application challenges of traditional law, and there are evidence gathering tracking challenges of identifying offenders.

While there are differences between court systems throughout the world, courts in democratic societies have some common characteristics. A court is an institution for finding solutions and making decisions in conflicts. In criminal law, there is a conflict between society and the offender.

Policing cybercrime remains a challenge as long as the police is organized along the geographical axis, while cybercrime occurs along the offence axis. There are no geographical distances on the Internet, while law enforcement is restricted by jurisdictions.

Prosecuting cybercrime remains a challenge as well, since the relevant jurisdiction is not always obvious. Some laws apply to citizens in a country independent of where the citizens committed their offences. Other laws apply only to citizens to the extent offences were committed within the relevant jurisdiction.