ARTICLE:

Evidence of cybercrime and coercive measures in Finland

By **Juhana Riekkinen**

Evidence of cybercrime – a dynamic, broad, and increasingly significant criminal phenomenon – differs from evidence of traditional crime. Accordingly, novel coercive measures, other investigatory powers, tactics, and technical methods are needed in order to secure evidence of cybercrime. In Finland, the new legislation on criminal investigations, coercive measures, and other police activities expressly regulates the searches of data and various other measures and powers that are useful in collecting evidence of cybercrime. While the current legislation seems to be mostly adequate, a balance between the efficiency of criminal investigations and the rights of the individual remains hard to find and uphold. Constant adjustments are required as criminality, technology, and societies continue to evolve.

Introduction

The rapid technological and societal developments that have taken us towards the network society have transformed the context of criminal evidence. Perhaps most significantly, a new criminal phenomenon, often labelled *cybercrime*, has emerged. Evidence of cybercrime is in many ways dissimilar to evidence of traditional forms of crime. Predominantly, it exists in digital and electronic form as *computer data*, which possesses numerous characteristics that separate it from traditional physical objects and documents.[1] Computer data (also 'data') is dependent on hardware and software, is voluminous, and more or less volatile. It can be easily transferred, copied, altered, forged, encrypted, damaged, or deleted – even without physical access to the device in which it is stored, intentionally or unintentionally. Potential electronic evidence is often spread over large geographical areas and across jurisdictional borders, and held or controlled by a number of different, sometimes not easily recognisable parties, such as the perpetrator, the victim, ISPs, and various other third parties.

Locating, obtaining, and preserving such electronic evidence in cybercrime investigations requires different tactics, methods, and tools from the law enforcement than the investigation of traditional crime.[2]

Coercive measures are vital legal instruments for law enforcement agencies. In addition to serving other interests related to guaranteeing the administration of justice, these legal instruments make the collection of evidence possible by various methods. Indeed, they play a major role in almost all criminal investigations. From the point of view of the targeted individual, however, coercive measures are often highly intrusive and violate their privacy-related rights, personal freedom, and other fundamental and human rights guaranteed in national constitutions and international conventions, most notably the European Convention on Human Rights ('ECHR') and the United Nations Covenants. Compliance with the measures may be literally coerced, by way of using physical force, if necessary.[3] Therefore, the use of coercive measures needs to be carefully regulated and paired with appropriate safeguards. The basic predicament of coercive measures comes down to finding a balance between the efficiency of criminal investigations and the rights of the individual.

In the age before computers and computer networks, the most central coercive measures for the purposes of evidence collection were those of *search* and *seizure*. These are indubitably still relevant, but translating the rules created for the physical world

[1] For a definition of computer data, see Council of Europe, *Convention on Cybercrime* (2001, ETS 185), Article 1(b) and *Explanatory Report to the Convention on Cybercrime* (2001), paragraph 25. The Convention is further addressed later in this paper.

[2] Generally about computer data as evidence, see, e.g., Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence in digital format', in *Electronic Evidence*, gen. ed. Stephen Mason (3rd edn, London: LexisNexis Butterworths, 2012), pp. 23–69. About investigating cybercrime, see, e.g., Robin Bryant and Ian Kennedy, 'Investigating Digital Crime', in *Policing Digital Crime*, ed. by Robin Bryant and Sarah Bryant (Farnham: Ashgate, 2014), pp. 123–145.

[3] In keeping with the Finnish legislative terminology, I also use the term 'coercive measure' in reference to covert coercive measures. These do not, due to their secretive nature, involve direct physical coercion (or even the threat of such coercion) of the targeted individual. Instead, covert coercive measures are executed without the knowledge of the targeted individual. All of the coercive measures that are addressed in this paper may also be classified as investigatory powers.

into the digital world has not been unproblematic, as has been observed in many jurisdictions. Furthermore, in the networked environment of today, the search and seizure of standalone devices is not sufficient to gather evidence of complicated forms of cybercrime. Various other types of coercive measures are needed, including measures for locating and identifying Internet users, data preservation orders, production orders, decryption orders, real-time interception of data and communications, technical surveillance, and other covert measures that make online investigations possible. The demand for new measures, together with the emphasis on the rights of the individual, has resulted in considerable increases in the volume and complexity of regulation on coercive measures.

This paper examines how evidence of modern cybercrime can be secured in compliance with the current legislative framework concerning coercive measures and other investigatory powers in Finland. The main component of this framework is the new Coercive Measures Act (806/2011, 'CMA'), which has been in effect since 1 January 2014, having replaced an older act of the same name. The Coercive Measures Act regulates the use of and the prerequisites for the use of coercive measures in criminal investigations, many of which may be used to collect evidence of an offence. Notably, the new act introduced a number of specific provisions on the search and surveillance of digital devices, and reinforced the status of the general principles of proportionality, minimum intervention, and sensitivity. Other relevant components of the framework are the Criminal Investigation Act (805/2011) and the Police Act (872/2011), which entered into effect simultaneously with the Coercive Measures Act. The Criminal Investigation Act governs, as the title suggests, how criminal investigations are conducted, whereas the Police Act contains, among other regulations, powers similar to coercive measures for the purposes of crime prevention and detection.[4] Special provisions on coercive measures and comparable powers are to be found in other legislation. The use of coercive measures is also linked to the material criminal law provisions in the Criminal Code (39/1889), and general procedural and evidentiary provisions found in the Code of Judicial Procedure (4/1734, 'CJP') and the Criminal Procedure Act (689/1997).[5]

The paper is structured as follows: the concept of cybercrime is clarified, and recent developments of cybercrime and associated challenges relating to evidence are described based on existing literature and reports; then the coercive measures authorised by Finnish law – the Coercive Measures Act in particular – that are relevant for the obtainment of evidence in cybercrime investigations are presented; this is followed by some observations in respect of the adequacy of currently available coercive measures, with attention also paid to the protection of the rights of the targeted individual. The article ends with conclusions and some final remarks.

Cybercrime and evidentiary challenges

Concept of cybercrime

Criminality connected to computers has existed since the 1960s, long before the first mass market personal computers (in the late 1970s) and the birth of the modern Internet and the World Wide Web (in the 1980s and 1990s). The term *cybercrime*, however, is more recent. It has gained popularity in connection with the rise of global computer networks, a development that has simultaneously escalated the scale and significance of the criminal phenomenon. Although cybercrime is now an everyday talking point, the terminology continues to be confusing and inconsistent, with notions such as computer crime, netcrime, Internet crime, e-Crime, and ICT crime being used in a largely interchangeable fashion. While most people probably have some instinctive idea of the meaning of these words, the concept of cybercrime remains rather ambiguous to this day. No commonly

[4] The relationship between the Coercive Measures Act and the Police Act – and, respectively, investigation and prevention and detection of offences – is somewhat complicated, and is not addressed in detail in this paper, which focuses on evidence collection in cybercrime investigations and therefore on the Coercive Measures Act.

[5] Unofficial translations of these (and approximately 600 other) acts are freely available on Finlex at http://www.finlex.fi/en/laki/kaannokset. General commentaries and textbooks on the Coercive Measures Act, the Criminal Investigation Act, and the Police Act are available in Finnish. They include Matti Tolvanen and Reima Kukkonen, *Esitutkinta- ja pakkokeino-oikeuden perusteet* (Helsinki: Talentum, 2011), Klaus Helminen and others, *Esitutkinta ja pakkokeinot* (5th edn, Helsinki: Talentum, 2014), Satu Rantaeskola (ed.), *Pakkokeinolaki – Kommentaari* (Tampere: Poliisiammattikorkeakoulu, 2014) http://urn.fi/URN:ISBN:978-951-815-279-1, Klaus Helminen, Matti Kuusimäki and Satu Rantaeskola, *Poliisilaki* (Helsinki: Talentum, 2012), and Satu Rantaeskola (ed.), *Poliisilaki – Kommentaari* (Tampere: Poliisiammattikorkeakoulu, 2014) http://urn.fi/URN:ISBN:978-951-815-286-9. Relevant sources of information also include the law drafting documents, in particular *Government Propositions 222/2010* and *224/2010*, freely available in Finnish and Swedish on *Finlex* and the Parliament website http://www.eduskunta.fi.

accepted, universal definition exists, and the exact demarcation of what constitutes a cybercrime and what does not is debatable.

This being said, there is a widespread consensus about the core meaning of the concept. By most understandings, cybercrime encompasses both entirely new forms of criminality as well as computer-assisted or computer-mediated versions of traditional crime. The factor that the new, cyber-specific crimes (e.g., computer break-ins and distributed denial-of-service attacks) and the old crimes applied to the network environment or conducted via a new medium (e.g., distribution of child pornography on P2P networks, e-mail frauds, and hate speech or threats on websites) have in common is some sort of a connection to ICT or computers. At its simplest, computer systems are usually either the instrument or the target of the crime.[6] A frequently used way of classifying and describing cybercrime is to make a division between *computer integrity, computer-assisted*, and *content-related* offences.[7] Whatever definition or typology is preferred,[8] it is notable that both the entirely new offences without a natural analogy in the physical world and the new versions of old offences may necessitate new criminal provisions, depending on how the pre-existing provisions are formulated.[9]

Recent developments

Cybercrime is not a static phenomenon. On the contrary, it is constantly evolving and transforming. Cybercrime today is very different from that of the early days of computers and computer networks. In general, cybercrime has become more organised and professional. In parallel, the economic influence of cybercrime has soared in recent years. It has been suggested that for criminals, cybercrime may be even more lucrative than traditional sectors of organised crime such as drugs, weapons, and human trafficking. On the other hand, these criminal activities are now increasingly connected to cybercrime and criminal marketplaces in cyberspace. This is linked to another line of development: cybercrime is increasingly connected to the physical world.

The *Internet Organised Crime Threat Assessment* (iOCTA) 2014 by Europol identified eight main crime areas: (1) crime-as-a-service, (2) malware, (3) child sexual exploitation online, (4) payment fraud, (5) criminal finances online, (6) crimes relating to social engineering, (7) data breaches and network intrusions, and (8) vulnerabilities of critical infrastructure.[10] A year later, a central finding in iOCTA 2015 was that cybercrime is becoming 'more aggressive and confrontational', with different forms of extortion becoming more common all the time.[11] Another illustration of the current situation is the report released by the Royal Canadian Mounted Police ('RCMP') in 2014, addressing cybercrime incidents and issues in Canada. This overview focused on examples and case studies on distributed denial of service attacks, criminal botnet operations, carding crimes, online mass-marketing fraud and ransomware, organised crime and the Internet, and online sexual exploitation. Further, the RCMP report described darknets, cybercrime-as-a-service, malware targeting mobile platforms, virtual currency schemes, cyber-facilitated stock market manipulation, and cybercrime threats to industrial control systems as

[6] For instance, see Dominik Brodowski and Felix C. Freiling, *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft* (Berlin: Forschungsforum Öffentliche Sicherheit, 2011), pp. 28–29 http://www.sicherheit-forschung.de/publikationen/schriftenreihe_neu/sr_kf/sr_4_kf.pdf

[7] See Jonathan Clough, *Principles of Cybercrime* (Cambridge: Cambridge University Press, 2010), pp. 9–11, and Ian Walden, 'Computer Crime and Information Misuse', in *Computer Law: The Law and Regulation of Information Technology*, ed. by Chris Reed and John Angel (6th edn, Oxford: Oxford University Press, 2007), pp. 553–554. A similar division is made in COM(2007) 267 final, p. 2.

[8] For other examples, see Ulrich Sieber, *Straftaten und Strafverfolgung im Internet* (München: Verlag C.H. Beck, 2012), pp. 18–35, Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, London: Routledge, 2012), pp. 101–103, Christopher L.T. Brown, *Computer Evidence: Collection and Preservation* (2nd edn, Boston: Cengage Learning, 2009), p. 13, Xingan Li, *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society* (Turku: University of Turku, 2008), pp. 112, 132–146, and Ernesto U. Savona and Mara Mignone, 'The Fox and the Hunters: How IC Technologies Change the Crime Race', in *Crime and Technology: New Frontiers for Regulations, Law Enforcement and Research*, ed. by Ernesto U. Savona (Dordrecht: Springer, 2004), pp. 11–14.

[9] About the difficulties of fitting new kinds of acts into the language of old provisions, see, for instance, Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, London: Routledge, 2012), pp. 114–117. About cyber-specific and general offences and national approaches to criminalisation of cybercrime, see UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 78–80 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[10] See Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2014* (2014), pp. 19–52 https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf.

[11] See Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2015* (2015), pp. 10, 62 https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf.

evolving cybercrime threats.[12] Based on both the iOCTA and RCMP reports, it can be said that cybercrime is a multi-faceted, complicated, and a developing problem.[13]

Evidentiary challenges in cybercrime investigations

Transnationality of cybercrime

Cybercrime has always been and is today a markedly and notoriously transnational and international phenomenon, owing to the fact that the structure of the Internet allows computer data to cross national borders swiftly and frequently. Purely domestic cybercrime does exist,[14] but according to the national responses to the United Nations Office of Drugs and Crime ('UNODC') cybercrime study, in the majority of countries, between 50 and 100 per cent of cybercriminal acts encountered by the police involve a transnational element.[15] If a suspected crime ever comes to the attention of any police force – the amount of undiscovered cybercrime (*Dunkelziffer*) is commonly estimated as being very high – the country in which the investigation is started may depend largely on chance.

From early on, the transnational character of cybercrime has been widely acknowledged,[16] and international cooperation in the field has been pursued extensively. Several legal instruments have been created. The focal points of the harmonisation efforts have been material criminal law, jurisdiction, and international cooperation. Some provisions on procedural powers, electronic evidence, and the responsibility of service providers have also been included in these instruments.[17]

The most significant and influential international treaty in the field is the Council of Europe *Convention on Cybercrime* (2001, ETS 185). An *Additional Protocol* to the Convention*, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (2003, ETS 189), has also been created. However, the Protocol has not been ratified as widely as the Convention itself. On the European level, the European Union's *Council Framework Decision 2005/222/JHA on attacks against information systems* and its successor, *Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*,[18] are noteworthy, as well. Finland has ratified both the Convention and the Additional Protocol. As a member of the EU, Finland has also implemented the EU instruments into national law.[19]

The Convention, the Additional Protocol and the EU instruments establish certain basic types of cybercrime offences that the parties (or member states) are required to criminalise. The offences covered by the instruments overlap, but the EU instruments are narrower in scope: they are limited to computer integrity crimes, whereas the Convention also contains computer-assisted and content-related offences.[20] Importantly, the Convention also sets requirements for national coercive measures (for which see articles 14-21). The main effect of the Directive, from the point of view of the topic of this paper, is that it requires more severe penalties for certain offences (see article 9). The defined criminal punishments affect the availability of coercive measures in the investigation of these offences – however, the actual changes brought by the

[12] See RCMP, *Cybercrime: An Overview of Incidents and Issues in Canada* (2014), pp. 8–13 http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada.
[13] See also Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, London: Routledge, 2012), pp. 101–102.
[14] This has been emphasised by Xingan Li, *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society* (Turku: University of Turku, 2008), p. 152.
[15] UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 117–118, 183–184. See also Dan Svantesson and Felicity Gerry, 'Access to extraterritorial evidence: The Microsoft cloud case and beyond', in *Computer Law & Security Review*, Vol. 31, Issue 4 (2015), pp. 483–484 http://dx.doi.org/10.1016/j.clsr.2015.05.007.
[16] UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), p. 5, cites a presentation at the Third INTERPOL Symposium on International Fraud, held in December 1979, as the earliest recognition of the 'international dimension'.
[17] For an overview of the most significant instruments, see UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 63–72.
[18] OJ L 69, 16.3.2005, p. 67–71.
[19] Finland ratified the Convention in May 2007, and related legislative amendments, which also satisfied the requirements of the Framework Decision, entered into effect in September 2007. The Additional Protocol was ratified in May 2011 and the necessary amendments entered into effect in September 2011. The Directive was implemented in September 2015.
[20] The Title headings in the Convention itself are 'Offences against the confidentiality, integrity and availability of computer data and systems', 'Computer-related offences', 'Content-related offences', and 'Offences related to infringements of copyright and related rights'.

implementation of the Directive were relatively minor in Finland.[21]

Evidence in electronic form

The evidence of cybercrime offences exists nearly exclusively in electronic form.[22] Eyewitness and earwitness testimonies and traditional physical evidence are rarely available. If they are, they must first be located through digital investigations, usually in the online environment. In contrast to traditional criminal investigations, electronic evidence is typically not just an additional element that can supplement other evidence, but an essential requirement for the success of the investigation and prosecution.

With the ever-increasing Internet traffic and storage capacity, as well as the duplicability and transferability of computer data, there is no shortage of potential electronic evidence. The sources are numerous, even if finding them may be challenging. Devices controlled, used, or abused by perpetrators of cybercrime often contain data that may be incriminating as evidence, such as e-mail messages, Internet browsing history, document files, media files, and system or application logs. Data connected with criminal activities can also be gathered from the public Web and third parties that offer online services and route, transmit, and control network traffic and data. Multiple copies of the very same data may be stored on different platforms and in several locations, creating opportunities for investigators.[23] However, the nature of data also allows for the swift destruction, hiding, obfuscation, and counterfeiting of that evidence. These problems are not limited to data stored on devices under the physical control of the perpetrator, because data stored in networked devices can be manipulated remotely.[24]

Perpetrators, of course, want to leave as little evidence of their actions as possible to be discovered by the investigators. When in danger of being caught, they will frequently try to delete any incriminating data; this may even be done automatically.[25] Although data 'deleted' via a normal operating system command is often recoverable, for a moderately knowledgeable person it is possible to wipe out – or physically destroy – the storage media in ways that leave little chance for even digital forensic specialists to recover anything worthwhile. A significant problem, besides the intentional destruction of data by perpetrators, is the fact that plenty of potentially useful data, especially data held by third parties or victims, is deleted or not stored at all because its significance is not recognised.

There are also ample of options for hiding data, some more efficient than others. Hidden folders, partitions, and unallocated hard disk slack space may be used for discreet storage. Relevant data may be concealed in seemingly innocuous files with the aid of steganography. Data may also be kept in external locations and on devices that are physically difficult to find and gain access to. Different kinds of password protection mechanisms may be used, or data may be encrypted, making it unintelligible to the investigators and anyone else without the information needed to decrypt it (usually a decryption key and an associated passphrase). Encryption of communications, messages, and individual files or folders causes difficulties for investigations and evidence collection, but a particularly problematic issue is the increasingly common use of full-disk encryption, which makes the entire contents of a suspect's computer or other digital device unreadable, thus eliminating a rich source of evidence. Although there are technical methods that can be used to try to decrypt encrypted data without the passphrase or decryption key, the encryption tools commonly available and used by cybercriminals are typically so strong that it is often impossible to gain access to the data in a reasonable timeframe.

Computer data is also alterable; it is easily modified knowingly or unknowingly. For skilled criminals, this can offer opportunities for forgery and manipulation

[21] See *Government Proposition 232/2014*, p. 6.
[22] UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), p. 122.
[23] Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence in digital format', in *Electronic Evidence*, gen. ed. Stephen Mason (3rd edn, London: LexisNexis Butterworths, 2012), p. 49, see also pp. 33–35.
[24] About anti-forensics, see Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence in digital format', in *Electronic Evidence*, gen. ed. Stephen Mason (3rd edn, London: LexisNexis Butterworths, 2012), pp. 53–68, Robin Bryant, Ed Day and Ian Kennedy, 'Opportunities and Challenges for the Future', in *Policing Digital Crime*, ed. by Robin Bryant and Sarah Bryant (Farnham: Ashgate, 2014), pp. 210–213, and Eoghan Casey, 'Computer Basics for Digital Investigators', in *Digital Evidence and Computer Crime*, by Eoghan Casey and contributors (3rd edn, Waltham: Academic Press, 2011), pp. 449–450, 456–462.
[25] A script or other software that reacts in some automated fashion to a specific triggering event, such as the loss of network connection, can be used to delete (or to hide) evidence. Such a script is sometimes referred to as a dead man's switch. Christopher L.T. Brown, *Computer Evidence: Collection and Preservation* (2nd edn, Boston: Cengage Learning, 2009), pp. 54, 68.

of evidence. On the other hand, this may mean that criminals leave behind traces that they are unaware of. From the point view of the investigators, even when the data can be accessed and gathered, great care must be exercised in the procedure and its documentation. For example, timestamps of a file, which could potentially prove an aspect of a criminal offence or link the suspect to the act, may be altered by actions performed during the search and analysis of the data. If the authenticity, integrity, or completeness of the data can be questioned, the evidentiary value of data may be severely impaired.[26]

Obscurity of the crime scene

In traditional criminal investigations with no immediately identifiable suspect, the point of departure is usually the physical crime scene. Criminal acts in the physical world can often be linked to a single location where the act was committed, and perhaps to one or a limited number of other, adjacent locations in which the effects of the act can be observed. These locations can then be searched for weapons, tools, objects, fingerprints, footprints, blood, skin cells, and various other kinds of physical tracks, traces, prints, and marks that can be forensically analysed. In contrast, in the network environment, the perpetrator of the act typically uses a device in one place, which may be anywhere in the world. As a result of a single click, data travels through various cables, routers, servers, and other devices, and brings about consequences in a wholly different location, or in a large number of locations, possibly distributed over a wide geographic area. The effects may even be observable from practically any device and location connected to the global network.

It is possible to conceptualise any computer or digital device linked to the crime as a *digital crime scene*, and valuable electronic evidence can be located by searching them.[27] However, even in the fortunate situation that all of these digital crime scenes are located inside the jurisdiction in which the investigation is pursued, they may be difficult to find. Investigators may not be able to identify a natural starting place for their investigation, especially if they have no identifiable suspect. In this context, however, it should be noted that cybercrime is a wide concept that covers numerous dissimilar acts. For instance, a reported computer break-in typically has an identifiable target and victim. In such a case, digital traces are usually scattered along the path from the target device to the perpetrator's device. That path may be long and complicated, but at least one of the ends is known to the investigators. Following the cyber trail may, ultimately, lead to the suspect and produce useful evidence. In the case of suspected distribution of copyrighted content through a P2P network, a different investigatory approach is required, as the copyright holders' locations are usually not relevant. Whether or not a clear physical starting location exists, information such as an IP address typically plays a major part in the early phases of the investigation. This heightens the importance of measures that allow investigators to receive subscriber information from ISPs or otherwise identify Internet users.[28]

Tracking the suspect and the attribution problem

If cybercrime takes place on the public Web, and if the perpetrator makes no effort in hiding their tracks, it is often relatively easy for the police, in cooperation with ISPs and website administrators,[29] to link the IP address to a person, household, or neighbourhood.[30] However, more dedicated cybercriminals use a wide range of methods for masking their identity, including the use of free access points, encryption, proxies, and onion routing in the form of anonymity networks such as Tor.[31] Much of the cybercriminal activity takes place

[26] Of course, even authentic, unaltered data may be unreliable or misleading for a variety of reasons, and should always be evaluated critically, as any other evidence. The evaluation of electronic evidence falls outside the scope of this paper.

[27] For more about the similarities and differences of such digital crime scenes and physical crime scenes, see Eoghan Casey and Bradley Schatz, 'Conducting Digital Investigations', in *Digital Evidence and Computer Crime*, by Eoghan Casey and contributors (3rd edn, Waltham: Academic Press, 2011), pp. 190–192.

[28] See UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), p. 143.

[29] About the interplay between investigators and private parties, see UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 144–152.

[30] ISPs usually possess data with which the IP address can be linked to a subscriber. In some cases, a static IP address is assigned to a specific person. The use of dynamic IP addresses, which are automatically allocated to users for a limited period of time, complicates the process somewhat, because the investigators have to find out who the IP address was allocated to at the time of the act. Even this is usually possible as the ISPs maintain records of IP allocation. UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 142–143 suggests that orders for subscriber information are the most commonly used investigatory power in cybercrime investigations.

[31] See Ulrich Sieber, *Straftaten und Strafverfolgung im Internet* (München: Verlag C.H. Beck, 2012), pp. 36–37. Specifically about Tor, see, e.g., Tor Project, *Tor: Overview* https://www.torproject.org/about/overview, and Tomáš Minárik and Anna-Maria Osula, 'Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law', in *Computer Law &*

hidden from the general public, on the Deep Web or the Darknet.[32] If a skilled perpetrator is determined to remain anonymous, tracking them becomes a task that requires high-level technical expertise and is time-consuming at best, impossible at worst. If the perpetrator operates from abroad, the process may be further complicated. Obtaining the necessary information from foreign ISPs may be slow and difficult. A specified form or procedure, or the cooperation of foreign authorities, may be required.[33]

If a suspect can be identified, locating them is a matter of normal police work, made easier by the fact that the IP address can often be linked to a physical address or location. Successively, the associated persons may be interrogated and other investigatory actions, such as searches, may be performed in appropriate locations. In effect, it is frequently the location that serves as the basis of identification, as it is easier to locate the device used to commit the crime than to identify the perpetrator. IP addresses, subscriber records, and other such information are crucial for a successful cybercrime investigation, but are insufficient on their own: several people may have access to the same device, and criminals frequently commit crimes remotely by exploiting security vulnerabilities and taking control of devices and network connections owned by others.[34] Indeed, one of the greatest challenges from the prosecutorial point of view is the attribution of the acts committed through an identifiable device to a specific person, which often requires a combination of many types of evidence.[35] Thus, locating the device seldom marks the end of an investigation.

Despite all the challenges in cybercrime investigations mentioned above, the standard of proof is not lower in cybercrime cases than in cases involving other offences.[36] According to Finnish law, a judgment of guilty may be made only on the condition that there is no reasonable doubt regarding the guilt of the defendant. The standard, which is modelled after the Anglo-American standard of *beyond reasonable doubt*, was recently codified in CJP, chapter 17 (732/2015), section 3(2).[37] Satisfying the standard of proof requires that the investigatory authorities have efficient and suitable legal powers of investigation and evidence collection. Otherwise, the challenges may become obstacles that cannot be overcome. Further, the lack of appropriate legal powers for investigating cybercrime may be in violation of human rights agreements.[38]

Security Review, Vol. 32, Issue 1 (2016), pp. 111–127 http://dx.doi.org/10.1016/j.clsr.2015.12.002.

[32] The Deep Web refers to the part of the Web that is not indexed by search engines. The Darknet refers to private, usually anonymous, distributed file sharing networks. Jessica Wood, 'The Darknet: A Digital Copyright Revolution', in *Richmond Journal of Law and Technology*, Vol. 16, Issue 4 (2010), pp. 16–19 http://jolt.richmond.edu/v16i4/article14.pdf. Generally, see Peter Biddle and others, 'The Darknet and the Future of Content Distribution', in *Digital Rights Management*, ed. by Joan Feigenbaum (Berlin/Heidelberg: Springer, 2003), pp. 155–176. See also RCMP, *Cybercrime: An Overview of Issues and Incidents in Canada* (2014), p. 13.

[33] About international requests for third parties, see UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), pp. 149–150. See also Dan Svantesson and Felicity Gerry, 'Access to extraterritorial evidence: The Microsoft cloud case and beyond', in *Computer Law & Security Review*, Vol. 31, Issue 4 (2015), pp. 478–489.

[34] About the evidentiary difficulties related to situations where Trojan horse programs are claimed to be the origin of criminal activity, see Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, London: Routledge, 2012), p. 125. In Nordic literature, the so-called 'Trojan Defense' and similar situations have been discussed by Inger Marie Sunde, 'Databevis', in *Bevis i straffesaker: Utvalgte emner*, ed. by Ragna Aarli, Mary-Ann Hedlund and Sverre Erik Jebens (Oslo: Gyldendal Juridisk, 2015), pp. 627–633.

[35] UNODC, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), p. 169. The attribution problem applies to electronic evidence of traditional crime, as well. See Eoghan Casey, 'Reconstructing Digital Evidence', in *Crime Reconstruction*, ed. by W. Jerry Chisum and Brent E. Turvey (Burlington: Academic Press, 2006), pp. 431–433.

[36] See the Finnish Supreme Court's decision *KKO 2013:96*, paragraph 5. The court stated that the standard of proof required in cases concerning sexual offences is not lower than the standard required in regard to other equally severe offences, even though the very nature of these acts often makes it difficult to obtain direct and unequivocal proof. There is no reason to assume that the court would treat cybercrime offences any differently than sexual offences. However, the court's position leaves open the possibility of the standard of proof varying according to the severity of the offence in question.

[37] A completely renewed chapter 17, concerning evidence, was passed by the Parliament along with related amendments to other legislation in 2015, and entered into effect on 1 January 2016. Even prior to this, Finnish courts had been using similar words to describe the standard of proof for well over ten years. See, e.g., the Supreme Court's decisions *KKO 2002:47*, *KKO 2004:60*, *KKO 2013:27*, and *KKO 2013:77*. See also *Government Proposition 46/2014*, p. 49, Pasi Pölönen and Antti Tapanila, *Todistelu oikeudenkäynnissä* (Helsinki: Tietosanoma, 2015), pp. 133–134, and Jaakko Rautio and Dan Frände, *Todistelu – Oikeudenkäymiskaaren 17 luvun kommentaari* (Helsinki: Edita, 2016), pp. 41–42.

[38] See, for instance, ECtHR, *K.U. v. Finland*, Judgment of 2 December 2008. The case concerned the lack of a measure to identify the person(s) who had placed an advertisement on an Internet dating site in the name of a 12-year-old boy without his knowledge. Although a suitable measure (Act on the Exercise of Freedom of Expression in Mass Media (460/2003), section 17) had been introduced by the time the case reached the ECtHR, the court held that there had been a violation of Article 8 of the ECHR, because the state had failed its positive obligation to protect the victim's right to respect for private life. For more about this case, see Tuomas Pöysti, 'Judgment in the case of *K.U. v Finland*: the European Court of Human Rights requires access to communications data to identify the sender to enable effective criminal prosecution in serious violations of private life', in 6 *Digital Evidence and Electronic Signature Law Review*, (2009), pp. 33–45.

Relevant coercive measures in Finnish law

Search

Search is a traditional, commonly utilised coercive measure for the purposes of finding and consequently obtaining objects and documents that may be usable as evidence. Searches of contents of digital devices differ somewhat from the traditional forms of physical searches. In some jurisdictions, old rules governing searches are applied to digital searches analogously, whereas in others cyber-specific rules have been created. The Convention on Cybercrime does not as such require specific rules concerning digital searches. Instead, it does require states to adopt such legislative and other measures as may be necessary to empower their competent authorities to search or similarly access computer systems and storage media (article 19(1), see also 19(2)). With the new Coercive Measures Act, Finland has adopted a partially cyber-specific legislative model.

CMA, chapter 8 contains provisions on different types of searches: *search of premises* (sections 1–19), *search of data contained in a device* (sections 20–29, 'search of data'), and *personal search* (sections 30–33). Searches of premises are further divided into three categories: (1) *general search of domestic premises*, (2) *special search of domestic premises*, and (3) *search of an area*. In this context, the concept of domestic premises gets its meaning by way of a reference to Criminal Code, chapter 24, section 11 (685/2009), which defines the concept of *domiciliary peace* for the purposes of criminal law, referred to in several criminal provisions located in the same chapter.[39] A search of domestic premises is 'special' when it can be assumed that the search would reveal information in respect of which a person is not permitted to or may refuse to testify in court proceedings, and in respect of which no seizure of a document may be directed. For instance, this covers the search of an attorney's or a doctor's home or offices. In these cases, the decision procedure is different, and a *search representative* needs to be appointed to ensure that seizure is not directed at privileged information.[40] The third category refers to searches in areas and places not protected by domiciliary peace, but which are not publicly accessibly or the public access to which is restricted or prevented at the time of the search. Moreover, searches of vehicles fall into this category. The three different categories of search of premises are also relevant in connection to the search of data.[41]

A search of data is defined in section 20(1) as 'a search that is directed at the data that is contained at the time of the search in a computer, a terminal end device or in another corresponding technical device or information system'. The scope of the provision is limited by section 20(2), which states that such a search may not be directed at a confidential message, in respect of which CMA, chapter 10 contains provisions on telecommunications interception, traffic data monitoring and technical surveillance. However, these covert measures apply to confidential messages *in transit*. Therefore, a (non-covert) search of data may be used to find and examine seizable e-mail and other messages that are stored on the device being searched, as clarified by an amendment to section

[39] As provided in this section, the criminal law concept of domestic premises covers homes, holiday homes and other premises intended for residential use, such as hotel rooms, tents, mobile homes and vessels with sleeping capacity, as well as the stairwells and corridors of residential buildings and the private yards of the residents and their immediate outbuildings. In Finnish constitutional law, the concept is more focused on premises intended for long-term residential use, and does not necessarily cover all the premises that are afforded protection in criminal law.

[40] See Markku Fredman, 'Erityinen kotietsintä ja etsintävaltuutetun tehtävät', in *Defensor Legis*, Vol. 95, Issue 2 (2014), pp. 155–177. See also ECtHR, *Sallinen and others v. Finland*, Judgment of 27 September 2005, which concerned the search and seizure of privileged material, including computer data, in a law office under the previous Coercive Measures Act, which did not recognise a similar special category of searches. The court held that there had been a violation of article 8 of the ECHR. This judgment and related national proceedings have been discussed in length by Finnish authors. See, e.g., Jaakko Rautio, 'KKO 2001:39 Takavarikkoratkaisun oikeusvoiman subjektiivinen ulottuvuus ja tietokonetiedosto takavarikko-objektina', in *KKO:n ratkaisut kommentein 2001:I*, ed. by Pekka Timonen (Helsinki: Kauppakaari, 2001), pp. 203–205, Markku Fredman, 'Kotietsintä ja takavarikko asianajotoimistossa', in *Defensor Legis*, Vol. 83, Issue 1 (2002), pp. 69–81, Pasi Pölönen, 'Asianajajan salassapitovelvollisuus asianajotoimistossa suoritettavassa takavarikossa', in *Defensor Legis*, Vol. 83, Issue 6 (2002), pp. 1044–1062, Jaakko Rautio, 'KKO 2002:85 Asianajajan tietokonetiedosto takavarikon kohteena', in *KKO:n ratkaisut kommentein 2002:II*, ed. by Pekka Timonen (Helsinki: Talentum, 2003), pp. 191–193, Pasi Pölönen, 'Petri Sallinen and others - tapaus', in *Defensor Legis*, Vol. 87, Issue 1 (2006), pp. 145–152, and Klaus Helminen and others, *Esitutkinta ja pakkokeinot* (5th edn, Helsinki: Talentum, 2014), pp. 985–987. For other ECtHR cases involving search and seizure of computer data in a law office, see *Smirnov v. Russia*, Judgment of 7 June 2007, and *Robathin v. Austria*, Judgment of 3 July 2012. See also *Saint-Paul Luxembourg S.A. v. Luxembourg*, Judgment of 18 April 2013, and *Nagla v. Latvia*, Judgment of 16 July 2013.

[41] Further, the purpose of the search of premises is legally relevant: the prerequisites for a search in order to find a person – not to be confused with a personal search, in which the target of the search is the person and the purpose of the search is to secure objects, documents, traces, etc. that they are carrying or have on them – differ from the prerequisites of a search in order to find an object or a document (see CMA, chapter 8, sections 2–4). This division is not relevant in relation to searches of data, as the *immediate* goal of such a search is – naturally – never to find a person but to find relevant data.

20(2) that was made prior to the Coercive Measures Act even entering into effect.[42]

A search of data may follow any type of a search of premises or a personal search, and it may also be conducted independently when the target device is otherwise accessible. In fact, this was one of the reasons why specific provisions on searches of data – previously thought to be covered by the general provisions on search of premises – were added to the law.[43] Although there are dissimilarities between the different types of search, there are also similarities. Consequently, according to the provisions of section 28, when a search of data is conducted in connection with a search of premises, the provisions on search of premises apply. Even in other situations, certain provisions that primarily concern searches of premises (on presence, procedure, the search representative, the opening and examination of a document, and the record) apply to searches of data as appropriate.

For the purposes of evidence collection, relevant prerequisites for a search of data are set out in section 21(1). First, there must be reason to suspect that a certain kind of offence has been committed. The most severe punishment provided for the offence (*in abstracto*, 'maximum punishment') must be imprisonment for at least six months, or, alternatively, the matter being investigated must involve circumstances connected to the imposition of a corporate fine. Second, it must be presumable that the search leads to the discovery of a document or data, which can be seized and which is connected with the offence under investigation.[44] These prerequisites highlight the connections between different types of searches, as they correspond to those of a search of domestic premises (section 2). In relation to the first requirement, searches of data are possible in investigations of most types of offences which enable the conduction of a search of the person (section 31) and all offences that enable the conduction of a bodily search (section 32).[45] Therefore, in most cases when a search of premises or a personal search results in finding a device or storage medium, a search of the data is also possible, providing it can be presumed to be fruitful.

Section 27 permits the carrying out of a search of data as a *remote search* – in other words, without using the device that is in the premises or in the possession of the person who is the subject of the search. This serves the speed and expediency of investigations in certain situations, when it is not necessary or practical to take physical possession of the device holding the data. However, Finnish law does not allow for covert online searches. Even when a search is carried out as a remote search, the general rules on notification and presence of the subject apply. Recently, the need for covert remote searches targeting computers and other devices has been suggested in public discussion.

In addition to material prerequisites, chapter 8 contains regulation on decision-making and procedure. Most decisions regarding searches can be made by an official with the power of arrest.[46] Concerning searches of premises, the relevant provision is section 15. The police do not need to obtain a judicial warrant for a general search of domestic premises or a search of an area. However, it is for the court to decide on a special search of a domicile and on the appointment of a search representative. In certain urgent situations, an official with the power of arrest may decide on a special search, and any police officer may conduct a general search or a search of an area. The same rules apply, as appropriate, to searches of data.

As a result of section 15, court authorisation is required *before the event* only for special searches of domestic premises in non-urgent situations, and correspondingly searches of data conducted along with these kinds of search. In addition, section 18 provides that a person whose domicile has been searched may challenge the legal validity of the search in court *after the event* within 30 days of the search, or of being informed of the search.[47] This possibility

[42] *Government Proposition 14/2013*, pp. 15, 41.
[43] *Government Proposition 222/2010*, p. 109.
[44] According to section 21(2), a search may also be conducted in order to return the device to a person entitled to it, if there are grounds to suspect that it has been taken from someone by an offence.
[45] The difference between these types of search is that a search under section 31 is limited to the clothes and possessions on the person, whereas section 32 includes searching body cavities and the taking of a blood sample or other sample.
[46] The officials with this power have been listed in CMA, chapter 2, section 9. They include police, border guard, and customs officials above a certain rank, as well as all prosecutors.
[47] This section was added after the ECtHR found that the Finnish law did not provide sufficient judicial safeguards either before the granting of a search warrant or after the search. See ECtHR, *Heino v Finland*, Judgment of 15 February 2011, and *Harju v Finland*, Judgment of 15 February 2011. As Markku Fredman, *Rikosasianajajan käsikirja* (Helsinki: Talentum, 2013), p. 488 critically remarks, the possibility to challenge the validity of the search had not yet been deemed necessary in *Government Proposition 222/2010*, despite the fact that the ECtHR had previously given similar judgments concerning other states.

does not apply when a search of data is conducted without connection to a search of domestic premises, as section 18 is not referred to in section 28.

Seizure

Once potential evidence has been located through investigatory methods and access to it has been gained, possibly by using coercive measures, it needs to be seized so that it can be further analysed and used as evidence in the trial. Traditionally, seizure meant confiscating an object or document by taking physical possession of the object or document. If the information contained in a document is relevant, sometimes it is not strictly necessary to use the original document in the latter phases of the proceedings. With photocopying technology, it has been possible to conveniently copy paper documents for a long time. Copying data is even more convenient and fast, but may also introduce legal and practical problems.

In Finland, the two alternative forms of seizure, confiscation and copying, are regulated in CMA, chapter 7.[48] Computer data can be seized either by copying it to a suitable storage medium, or by physically confiscating the original storage medium or the entire computer device. When it comes to documents, according to section 2(1), copying is the primary option if a copy is sufficient from the point of view of the credibility and reliability of evidence. In cybercrime investigations, however, it is commonly necessary to both confiscate the original storage medium and to create a bit-for-bit copy of the contents for the purposes of a digital forensics investigation. It should be noted that copying typically requires physical possession for a short term, except, for instance, when searches of data are conducted remotely. Whenever copying cannot be conducted without delay due to the nature or extent of the document or documentation, the document – in practice, the storage medium or the computer device – must be confiscated.

In a typical criminal investigation, a seizure typically follows some type of a search. First, an object of interest is located in a search, and consequently, the authorities take it into their possession in order to secure its future use as evidence in the trial, or for some other purpose (e.g., to return the object to its rightful owner). Seizures are, however, not limited to these post-search situations, but can also relate to other coercive measures and situations. Nevertheless, the prerequisites for different kinds of searches largely determine when a seizure is possible. The prerequisites for seizure itself are not difficult to meet – according to section 1(1), an object, property or document may be seized if there are grounds to suspect that it may be used as evidence in a criminal case.[49] There are no further specific material prerequisites, but the general principles of proportionality and minimum intervention need to be taken into account. As regards the procedure, no judicial warrant is needed *before the event*; the decision-making power generally rests with an official with the power of arrest. The seizure may be later challenged in court, and the court may rescind the confiscation and order the copies to be deleted. When considering charges, the court may also make the original decision on seizure.

As stipulated by section 3, there are some prohibitions on seizure corresponding to various privileges that require or allow a person to refuse to testify. For example, a document which contains information covered by the attorney-client privilege or the medical professional privilege may not be seized to be used as evidence.[50] The prohibitions on seizure are not absolute, insofar that they do not apply in circumstances under which the respective privilege can be removed by the court at trial, or if the person protected by such privilege consents to the seizure.[51] Furthermore, section 4 prohibits the seizure

[48] In this paper, the term seizure is used as a collective term referring both to the physical confiscation of an object or a document, and to the copying of a document. No such all-encompassing term is used in the Act itself. Confiscation and copying are regulated in the same chapter and to a large extent, the same rules apply to both of them. In the Convention on Cybercrime, the powers relating to seizure of computer data are regulated in Article 19(3). The expression 'seize or similarly secure' is used in sub-paragraph a, whereas the power to 'make and retain a copy of those computer data' is separately mentioned in sub-paragraph b.

[49] Additionally, confiscation is possible if there are grounds to suspect that the property or document has been taken from someone in an offence, or may be ordered forfeited. Notably, the last of these grounds does not apply to data, as stated in section 1(2).

[50] See CJP, chapter 17, sections 10–14, 16, 20, and 21. These privileges are discussed in detail by Pasi Pölönen and Antti Tapanila, *Todistelu oikeudenkäynnissä* (Helsinki: Tietosanoma, 2015), pp. 278–321, and Jaakko Rautio and Dan Frände, *Todistelu – Oikeudenkäymiskaaren 17 luvun kommentaari* (Helsinki: Edita, 2016), pp. 91–161.

[51] For example, the attorney-client privilege (except when it comes to criminal defence lawyers) and the medical professional privilege can be removed at trial if the maximum punishment for the offence is imprisonment for at least six years. If the court makes such a decision, the respective obligation to refuse to testify ceases to apply. Consequently, the witness is obliged to testify, and privileged information can be presented as evidence.

of a document or data in the possession of a telecommunications operator or a corporate or association subscriber, if it contains data related to a message, identifying data, or base station data. These kinds of data need to be secured by using covert measures regulated in Chapter 10, the use of which is more limited than that of a regular seizure.

Preservation orders and data retention obligations

Electronic evidence is often in the possession of third parties. Unfortunately, computer data is volatile; potential electronic evidence is often lost or damaged irreparably before it is found and collected by the authorities. Due to both legal and practical reasons, gaining access to relevant data that is in the possession of third parties may take a considerable amount of time, especially in transnational investigations. Data preservation (or data retention) orders may be useful in making sure that the data still exists when the authorities are able to get to it.

The Convention on Cybercrime does not specifically oblige the parties to adopt data preservation orders. Preservation orders are, however, mentioned as an example of means to obtain the expeditious preservation of specified computer data (article 16). In Finland, data preservation orders were first inserted to the previous Coercive Measures Act (450/1987) in 2007, following the ratification of the Convention. In the previous Act, they were placed in the chapter governing seizure. Currently, data preservation orders are regulated in CMA, chapter 8, sections 24–26, along with the provisions regarding search of data.

As provided in section 24(1), if, prior to a search of data, there is reason to assume that data that may be of significance for the clarification of the offence is deleted or is changed, a data preservation order may be issued by an official with the power of arrest. Such an order obliges the receiver – a person holding or administering data, but not the suspect – to maintain the data unchanged. A data preservation order may be issued in advance, applying to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. This represents a change from the earlier law, which did not allow for such pre-emptive preservation orders. Whether or not the data in question already exists or not, a written certificate must be given on request, and the object of preservation must be identified and detailed with such accuracy that the order can be complied with.

Section 24(2) states that preservation orders can also be directed at transmission data, defined in the same provision as 'data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time, duration, nature and other corresponding factors of the transmission'. The provisions of section 24(3) provide that the authorities do not, on the basis of the preservation order, have the right to obtain information on the contents of the message, transmission information, or other recorded information. As an exception, if several service providers have participated in the transmission of the message referred to in subsection 2, the authorities have the right to obtain the transmission information necessary to identify the service providers.[52]

Section 25 provides that a data preservation order may be issued for three months at a time. The order may be renewed when required by the investigation of the offence, and it must be rescinded as soon as it is no longer necessary. Section 26 contains a secrecy obligation, which applies to the person who has received a data preservation order. The violation of the secrecy obligation is a criminal offence.

In addition to the possibility of data preservation orders in a specific case, Finnish law – currently chapter 19, sections 157-159 of the new Information Society Code (917/2014) – provides for a general obligation of service providers to retain traffic data for a specified time.[53] The data retention obligation applies to traffic data related to three different kinds of services: (1) telephone services or SMS services, (2) Internet telephone services, and (3) Internet access services. The retention times for the three groups of traffic data are twelve, six, and nine months, respectively. The use of the retained data is only permissible in the clarification of the offences defined in CMA, chapter 10, section 6(2). The referred provision states that *traffic data monitoring* may be conducted when there are grounds to suspect a

[52] This exception is related to the technical functioning of computer networks, as elaborated in *Government Proposition 153/2006*, p. 72.
[53] The obligation applies to 'an undertaking designated by a separate decision of the Ministry of the Interior that has submitted a telecommunications notification', and it does not include an obligation to generate any data but merely to retain data that is generated for other purposes.

person of certain offences. These offences include all offences committed with the use of a network address or terminal end device for which the maximum punishment is imprisonment for at least two years. For other offences, the general prerequisite is four years.

Production and decryption of computer data

In Finnish law, there are no specific provisions on orders for the production of computer data.[54] Thus, the general rules concerning the obligation of a witness to produce evidence apply also to computer data. In fact, article 18 of the Convention on Cybercrime was implemented not by adding specific norms on the production of computer data, but by clarifying the general provision on the production of evidence in criminal investigations.[55] A similar obligation exists also in the trial phase.[56] Additionally, during trial, the court may order an object or a document to be brought to the court if it may be relevant as evidence.[57] The obligations do not apply to suspects, and persons who have the right or duty to refuse to testify are not obliged to produce evidence that contains privileged information. Correspondingly, the court cannot order such persons to produce this kind of object, document, or data. The norms relating to production of data are not connected to any special requirements besides the relevance of the data as evidence.

As previously mentioned, encrypted data that may be useful as evidence of a cybercrime is currently a major issue faced by criminal investigators. Finnish law contains no provisions on explicit decryption orders, but follows the example of the Convention on Cybercrime, article 19(4). Pursuant to CMA, chapter 8, section 23(1), a person possessing or maintaining an information system or other person is required to provide to a criminal investigation authority at its request *the passwords and other corresponding information necessary to conduct the search of data*. On request, a written certificate shall be given to the person to whom the request was made. If a person refuses, they can be heard in court and consequently sanctioned, if necessary. This provision applies to decryption keys and related passphrases and therefore works as a decryption order. Again, as stated in section 23(3), the obligation does not apply to the suspect – who is the person most likely to be able to decrypt the data – or persons who have the right or duty to refuse to testify, and therefore they cannot be ordered to decrypt their data under threat of criminal or other sanctions.[58] No further prerequisites are provided for the obligation to provide the information necessary to conduct the search of data. Such an obligation is naturally tied to the prerequisites of a search of data, described above. Additionally, according to CMA, chapter 10, section 50, the provisions concerning this obligation apply in the use of covert coercive measures, which involve considerably stricter prerequisites, described below.

Covert coercive measures

General

Covert coercive measures for the purposes of criminal investigations are regulated in CMA, chapter 10. A nearly identical regulation for the purposes of crime prevention and detection is contained in Police Act, chapter 5. Since the early 1990s, the amount of regulation on covert coercive measures and surveillance has significantly increased. The development has affected not only the number of provisions granting the police authorisation for various actions, but also the number of provisions designed to guarantee the rights of the targeted individuals. As a result, the regulation of covert coercive measures has become a wide-ranging and complicated field that cannot be presented comprehensively in the limits of this paper.[59] The

[54] Concerning the release of identifying information for a network message, however, see Act on the Exercise of Freedom of Expression in Mass Media, section 17 (906/2015). In obtaining identifying information, also Police Act, chapter 4, section 3 can be used as a basis.
[55] The amended provision was section 27 of the previous Criminal Investigation Act (449/1987). Currently, the obligation is based on Criminal Investigation Act, chapter 7, section 8(3).
[56] The current provision containing the general obligation, regarding both objects and documents, is CJP, chapter 17, section 9. Before the renewal of chapter 17, the relevant sections were 12–17 (concerning documents) and 57 (concerning objects, with reference to sections 13–17).
[57] This is explicitly stated in the current CJP, chapter 17, section 40.

[58] Therefore the Finnish law largely differs from England and Wales, where decryption orders may be issued at suspects under Regulation of Investigatory Powers Act of 2000, Part III, under the threat of a criminal penalty. See Stephen Mason, 'Encrypted Data', in *Electronic Evidence*, gen. ed. Stephen Mason (3rd edn, London: LexisNexis Butterworths, 2012), pp. 195–200, 206–216.
[59] Recently, a considerable amount of attention has been given to covert coercive measures and surveillance both by the Finnish media and legal scholars. General, recently published accounts (in Finnish) on the topic are Klaus Helminen, Matti Kuusimäki and Satu Rantaeskola, *Poliisilaki* (Helsinki: Talentum, 2012), pp. 385–430, Markku Fredman, *Rikosasianajajan käsikirja* (Helsinki: Talentum, 2013), pp. 518–539, Klaus Helminen and others, *Esitutkinta ja pakkokeinot* (5th edn, Helsinki: Talentum, 2014), pp. 1103–1265, Arto Hankilanoja, *Poliisin salainen tiedonhankinta* (Helsinki:

following is meant as a brief overview. Emphasis is placed on select measures that are principally relevant in this context, in particular measures that allow for the collection of electronic evidence from computer devices and networks.

Generally speaking, covert coercive measures are more invasive than other coercive measures because of their secretive nature; the targeted individuals do not know that they are being subjected to surveillance, and thus cannot object or react to the measure. Nevertheless, covert measures have been seen as necessary in tackling serious crime. To solve this predicament, these highly invasive measures need to be matched with particularly effective safeguards, checks, and balances. In Finland, as a general rule, a court makes decisions on the use of covert coercive measures. In contrast to searches, a judicial warrant is often required in advance. The use of covert coercive measures is also otherwise more limited, and usually possible only in investigations involving serious offences. Some general prerequisites for the use of covert coercive measures are set in CMA, chapter 10, section 2.[60] Specific prerequisites, which vary depending on the invasiveness and other qualities of the measure, are set in provisions concerning each individual measure.

The coercive measures currently authorised by chapter 10 can be divided into three basic categories: (1) *coercive telecommunications measures*, (2) *surveillance-like coercive measures*, and (3) *special covert coercive measures*. All of the categories are potentially relevant from the viewpoint of evidence collection in cybercrime investigations.

Coercive telecommunications measures

Coercive telecommunications measures include telecommunications interception and the obtaining of information other than through telecommunications interception[61] (sections 3–5), traffic data monitoring (sections 6, 7 and 9), and obtaining base station data (sections 10 and 11).[62] In general, the measures are used to gather information about *private communication* in *public communication networks*. Telecommunications measures are, to a certain extent, technologically neutral. Thus, these powers, which also satisfy the requirements of the Convention on Cybercrime, articles 20 and 21, are equally applicable to telephone calls, VoIP calls, e-mails, instant messages, and even private messages on social media services. An important notion, however, is that the intrusiveness of seemingly neutral measures may differ depending on the technology.[63]

The prerequisites for the use of telecommunications measures are relatively high. Consequently, telecommunications measures are often not available in investigations of less serious forms of cybercrime. In particular, this applies to the interception of telecommunications, which may be permitted only when the suspected offence is one of the offences listed in section 3. Interception of telecommunications

Talentum, 2014), and Tuomas Metsäranta, *Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja* (Turku: University of Turku, 2015) http://urn.fi/URN:ISBN:978-951-29-6068-2. See also Pasi Pölönen, 'Salaisista pakkokeinoista ja tiedustelutoiminnasta' in *Lakimies*, Vol. 95, Issue 8 (1997), pp. 1206–1232, Rauno Korhonen, *Poliisin valvontakeinot ja kansalaisten yksityisyyden suoja* (Helsinki: Edita, 2005), pp. 97–103, 123–179, and Johanna Niemi and Virve-Maria de Godzinsky, *Telepakkokeinojen oikeussuojajärjestelmä* (Helsinki: Oikeuspoliittinen tutkimuslaitos, 2009).

[60] According to CMA, chapter 10, section 2(1), a general prerequisite for the use of all covert coercive measures is that their use may be assumed to produce information needed to clarify an offence. Additionally, section 2(2) provides for extra prerequisites for more invasive groups of measures: Telecommunications interception, the obtaining of data other than through telecommunications interception, extended surveillance, on-site interception, technical observation, technical monitoring of a person, technical surveillance of a device, covert activity, pseudo-purchase, the use of covert human intelligence sources, and controlled delivery may be used only if they can be assumed to be of particularly important significance in the clarification of an offence. An additional prerequisite for the use of covert activity, pseudo-purchase, and on-site interception in domestic premises is that this is *necessary* for the clarification of an offence. The corresponding Police Act provisions (chapter 5, sections 2(1) and 2(2)) refer to prevention or detection of an offence instead of clarification. As suggested by Tuomas Metsäranta, *Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja* (Turku: University of Turku, 2015), pp. 193–197, the protection afforded by these general prerequisites and the added value of the three-tiered system is questionable.

[61] The prerequisites for the latter, rather cryptically named measure are the same as for telecommunications interception. In accordance with section 4, it can refer to seizing messages from third parties after the communication has taken place when the message and the identifying data are no longer available through actual telecommunications interception. The section also covers the interception of a signal between a 'personal technical device that is suitable for sending and receiving a message and that is directly connected to a terminal end device' and a terminal end device used for communications; for example, between a Bluetooth headset used by the suspect and the suspect's cell telephone. Under the same section, interception may also be directed at the personal technical device itself.

[62] Additionally, investigatory authorities may obtain location data in order to contact a suspect or a convicted person (sections 8–9). This power has little or no relevance from the point of view of evidence collection.

[63] As an example, although both IP addresses and telephone numbers are considered identifying data and may be collected under the same rules on traffic data monitoring, IP addresses are often far more revealing as regards the content of Internet communications and other online activities than phone numbers are as regards the content of a telephone conversation. When combined with other data, IP addresses reveal information about a wide range of online behaviour, not just communication between natural persons.

allows for the monitoring, recording, and processing of the message itself, as opposed to only identifying data or location data, and therefore it is the most invasive telecommunications measure. Almost all typical cybercrime offences fall outside the scope of the measure, including even relatively serious offences such as aggravated forms of *interference with communications*, *interference in an information system*, and *computer break-in*.[64] Notable exceptions are *aggravated distribution of a sexually offensive picture depicting a child*, and since September 2015, the newly created offence of *aggravated damage to data*.[65] In general, the measure is available only in investigations involving very serious offences having to do with national security, health and lives of individuals, and certain other serious offences relating to organised and economic crime.

In comparison, traffic data monitoring is much more widely available in cybercrime investigations. There is a special lowered prerequisite that applies to most forms of cybercrime; in an investigation of an offence committed with the use of a network address or terminal end device, the prerequisite of maximum punishment for the suspected offence is imprisonment for at least two years, as opposed to the general limit of four years (section 6(2)). This covers offences such as *interference with communications*, *interference in an information system*, *computer break-in*, *damage to data*, and *endangerment of data processing*, as well as the computer-assisted forms of *fraud, forgery* and *aggravated defamation*. A further exception is made for *unauthorised use* directed at an automatic data processing system, for which the maximum punishment is imprisonment for one year only. Additionally, with the consent of the possessor of a network address or terminal end device, traffic data monitoring is permissible in virtually all cybercrime investigations under section 7(1).

A warrant issued by a judge is always required for the interception of telecommunications. As for traffic data monitoring and obtaining base station data, a judicial warrant is generally needed, but there are some exceptions. The first exception concerns situations of urgency, in which an official with the power of arrest may make a temporary decision, to be subjected to judicial review afterwards. The second exception applies to consent-based traffic data monitoring in some specific situations.[66] In this case, the final decision may be made by an official with the power of arrest.

Surveillance-like coercive measures

Surveillance-like coercive measures include on-site interception (sections 16–18), technical observation (sections 19 and 20), and technical monitoring (sections 21 and 22). However, perhaps the most interesting measure in respect of cybercrime investigations is *technical surveillance of a device* (sections 23 and 24), which may be used for the surveillance of digital devices such as desktop computers, laptops, tablets, or smartphones. Technical surveillance of a device is defined in section 23(1) as 'other than solely sensory surveillance, recording or other processing of the operation of a computer or other corresponding technical device or of the data or identification data contained therein, for the purpose of the investigation of a factor that is of significance for the clarification of an offence.' The measure must be directed at a device or its program that is *probably used by the suspect*. Therefore, surveillance may under some circumstances be legally directed at a device which is not *owned* by the subject. If it becomes evident that the device is not used by the suspect, the measure must be interrupted and the records and notes must be destroyed. A notable limitation is set in section 23(2), which prohibits the use of this measure as a replacement of telecommunications interception and traffic data monitoring in order to obtain information about the content of a message or identifying data, which is only possible under their respective prerequisites. Section 58 further provides that if it becomes evident that the surveillance is directed at such data, the measure must be interrupted and already gathered records and notes must be destroyed.

Technical surveillance of a device may be conducted if there are grounds to suspect someone of an offence for which the maximum punishment is imprisonment for at least four years, or for a small number of other

[64] These offences are all located in Criminal Code, chapter 38. After amendment 368/2015, the maximum punishments for the offences are five, five, and three years, respectively. The list in CMA, chapter 10, section 3 includes several offences with comparable or even lower maximum punishments.

[65] The relevant penal provisions are Criminal Code, chapter 17, section 18(a) (650/2004) and chapter 35, section 3(b) (368/2015). Before the creation of the new provisions concerning damage to data, similar actions fell under section 2 of the same chapter, which defines a more general offence of *aggravated criminal damage*. This offence was—and is—included in CMA, chapter 10, section 3.

[66] See section 7(1), paragraphs 2 and 3.

listed offences. The list does not include offences committed with the use of a network address or a terminal end device.[67] The general limit of four years covers aggravated forms of the above-mentioned offences such as *interference with communications*, *interference in an information system*, *damage to data*, *fraud*, and *forgery*. This means that technical surveillance of a device is permissible more rarely than traffic data monitoring, although much more often than interception of telecommunications.

Technical surveillance of a device may be carried out by, for example, installing a key-logger or remote-viewing software on the subjected device. Alternatively, a specific device may be installed for the same purpose. Installation of *devices*, *procedures*, and *programs* in the object, substance, property, premises, or other place that is targeted by any form of technical surveillance is expressly authorised in section 26. This also means that any digital device and computer system used by the suspect may be made to record sound, images, or location data by breaking into it and installing software that is largely similar to spyware and malware used by cybercriminals. When used by the police or other governmental agencies, this kind of software is sometimes dubbed *policeware* or *govware*.

In addition to technical surveillance, surveillance-like coercive measures include extended surveillance (sections 12 and 13). Extended surveillance, as provided in section 12(2), refers to *other than short-term surveillance* of a suspect in an offence, and is subject to prerequisites defined in sections 12(3) and 12(4). Short-term, covert observation of a certain person for the purpose of collection of intelligence is not a specifically regulated coercive measure, and the police are authorised to conduct such surveillance without any special prerequisites (or, apparently, even the general prerequisites of covert coercive measures defined in section 2).[68] The observer may use technical devices such as binoculars and cameras. Despite the fact that the primary form of surveillance is the sensory observation of a person in the physical world, analogous observation may be conducted in computer networks. For example, the police may read messages posted on a publicly available Internet bulletin board or other website without any prerequisites.[69] However, due to the definition of extended surveillance, it seems that a more extensive, continuous, or long-term surveillance of a suspect's online behaviour on public websites demands that the prerequisites of extended surveillance are met.

Decision-making on surveillance-like coercive measures varies in connection with the intrusiveness of the measure. For on-site interception, technical observation, technical monitoring of an individual, and technical surveillance of a device, a judicial warrant is generally required. As regards the latter two, in situations of urgency, an individual with the power of arrest may make temporary decisions to be subjected to judicial review afterwards. Additionally, an official with the power of arrest may decide to undertake on-site interception and technical observation outside domestic premises when these measures are not directed at a person who has lost his or her liberty as a result of an offence. An official with the power of arrest may also decide on technical monitoring of other than an individual, as well as on extended surveillance.

Special covert coercive measures

Of the special covert coercive measures, covert activity (sections 27-33) is particularly noteworthy in cybercrime investigations. In contrast to the measures of passive surveillance, covert activity involves interaction with suspects and other persons and even infiltration. In accordance with the definition in section 27(1), covert activity refers to the extended collection of intelligence directed at a certain person or at his or her activity through the use of infiltration, in which false, misleading or concealed information or register notations are used or false documents are prepared or used, in order to achieve the confidence needed for the collection of intelligence or to prevent the revelation of the collection of intelligence.

Interestingly for cybercrime investigations, section 27(3) explicitly recognises the possibility of covert activity over a computer network. This kind of online covert activity is allowed if there are grounds to suspect the targeted person of an offence for which

[67] Section 23(3) refers to offences defined in section 16(3), which concerns the prerequisites of on-site interception. The listed offences are *narcotics offence*, *preparation of an offence committed with terrorist intent*, *aggravated customs offence*, *preparation of the taking of a hostage*, and *preparation of aggravated robbery*. While these offences are not cybercrime per se, they may be conducted online with the aid of computer systems.

[68] The definition of surveillance is provided in CMA, chapter 10, section 12(1) mainly in order to more accurately define the coercive measure of extended surveillance.

[69] *Government Proposition 222/2010*, p. 325. Posts on public websites are not protected as *private* communication.

the maximum punishment is imprisonment for at least two years or if the offence in question is *possession of a sexually offensive picture depicting a child*, which is punishable by fine or imprisonment for at most one year. In contrast, the use of covert activity outside the network environment is as strictly limited as that of telecommunications interception, with some exceptions stated in section 27(2). As regards cybercrime, the relevant exception is that when the suspected offence is *distribution of a sexually offensive picture* depicting a child, covert activity is permissible but telecommunications interception is not.[70]

Curiously, a similar lowered maximum punishment prerequisite is not provided in the law in respect of online covert collection of intelligence (sections 14 and 15). This measure also involves interaction, and is, essentially, a short-term, 'light' version of covert activity without the infiltration component.[71] As a consequence, covert activity may – somewhat illogically – be permissible in online cybercrime investigations when covert collection of intelligence is not.

In certain situations, also pseudo-purchases (sections 34-37), covert human intelligence sources (sections 39 and 40), and controlled deliveries (sections 41 and 42) may be used to gather evidence in cybercrime investigations. However, there is no special regulation relating to the network environment or cybercrime. Decisions on special covert coercive measures are made by high-ranking officials inside the police organisation, such as the chief of the National Bureau of Investigation. Decisions on some of the less invasive measures, including covert collection of intelligence and online covert activity, may be made by an official with the power of arrest who has been particularly trained in covert collection of intelligence and who has been appointed to the task.

Adequacy of the current law

On a basic level, all of the coercive measures regulated in the Coercive Measures Act may be used in cybercrime investigations.[72] However, not all of the measures may be used in all cybercrime investigations and in all situations. Whether a measure is permissible depends on the quality of the offence under investigation and the specific prerequisites of use concerning each measure. Further, some measures are not particularly useful in collecting evidence in cybercrime investigations, whereas others – mainly those that can be used to collect electronic evidence – are especially valuable in cybercrime investigations.

The prerequisites for search and seizure are comparatively low in Finland. This holds true also in the digital environment. No judicial warrant is required for a search of premises or a personal search through which a device can be located, or for a search of the data contained in the device, with the exception of special searches of premises and associated searches of data. The maximum punishment prerequisite of six months allows for searches, both physical and digital, to be conducted in investigations of most cybercrime offences, save for some petty offences and violations that are punishable with a fine only. With the current legislation, there is also some flexibility to how the search can be carried out; remote searches are possible, albeit not covertly. Seizure is permissible in the investigation of any suspected offence, practically always when it is necessary or beneficial. The only significant limitations for the use of seizure are the prohibitions concerning privileged information and the general principles of proportionality and minimum intervention, also embodied by the primacy of copying over confiscation. The emphasis on these principles may also lead to problems with deciding whether to copy data, because the best digital forensic practice usually demands a bit-for-bit copy of the entire storage medium, even when the material of interest may only form a very small part of the data stored on the medium in question.

Ordered preservation, production, and decryption of data are treated differently in Finnish law. For preservation orders, there is a clear regulation that is specific to computer data. Curiously, this power is

[70] Criminal Code, chapter 17, section 18 (650/2004) criminalises the distribution of sexually offensive pictures depicting children, violence, and bestiality. The punishment is fine or imprisonment for at most two years.

[71] Compare the definition of covert activity, quoted above, with CMA, chapter 10, section 12(1): 'Covert collection of intelligence refers to short-term interaction with a certain person for the obtaining of information, and in which a police officer in order to conceal the task uses false, misleading or concealed information.'

[72] The coercive measure of *on-site interception in domestic premises* (CMA, chapter 10, section 17) is not permissible in the investigation of any offences addressed by the Convention on Cybercrime. Of the offences listed in the section, however, for example *aggravated narcotics offence* may be committed with the aid of computer networks (e.g., via online marketplaces in the Darknet). Also other listed offences, such as *aggravated sexual abuse of a child*, various terrorism-related offences, and even *murder*, may be committed through computer systems and network connections.

strongly linked to searches of data instead of an order to produce data, which is often a better alternative when electronic evidence is held by a third party that is able and willing to cooperate. Production, on the other hand, is not regulated computer-specifically at all. The existing legislation seems to provide the necessary means for ordering the production of computer data from a third party, but it is conceivable that the cost-efficiency and the reliability of the produced data could be improved with specific legislation or guidelines addressing the specific characteristics of electronic evidence. If third parties had clear, legally validated procedures to follow in the event that they possess relevant data (e.g., for maintaining and documenting the continuity of evidence – also known as chain-of-custody – and the integrity of the data), there would be less need for the investigatory authorities to perform searches of data on third parties.

Encryption of data, which is a substantial problem in cybercrime investigations, has not been addressed in detail by the Finnish legislators. In practise, there is a possibility to order a third party to provide the information needed to decrypt or otherwise provide access to computer data. There are no additional material prerequisites for this kind of warrant. Hence, decryption can be ordered any time a lawful search or other coercive measure brings to attention encrypted data. It remains somewhat unclear – and untested in Finnish courts – how far the co-operating private party may be obligated to go in order to accommodate the request. The Finnish provision does not contain the limitation clause 'as is reasonable', which is present in the Convention on Cybercrime, article 19(4). Nevertheless, the background and the wording of the section strongly suggest that the obligation cannot be stretched so that a private software or hardware provider could be ordered to create a specific new tool for the purpose of decrypting the data in question, or to create a backdoor in their encryption software, operating system, or other such product that the suspect of a criminal investigation is using.[73]

Yet, the main problem of decryption orders is still that third parties are rarely in any position to provide the information needed to decrypt the data. This is routinely the situation if the perpetrator of cybercrime has encrypted their data on purpose. Although suspects cannot be forced to provide self-incriminating information, covert coercive measures – technical surveillance of a device, in particular – may be helpful in obtaining the information needed to decrypt data from the suspect themselves. The use of these measures, however, is considerably more limited.

Indeed, Finnish law does authorise numerous covert coercive measures that may be of use in cybercrime investigations. The prerequisites for the use of these measures are high compared to the prerequisites for search, seizure, or other non-covert measures. Covert coercive measures are permitted only in the investigation of relatively serious criminal offences, which are defined using varying legislative techniques. Rightly so, there are some lowered thresholds for cybercrime; the covert surveillance of online activities that are likely to be directly related to the suspected cybercrime offence can be seen as more justified than the surveillance of online activities that may be entirely unrelated to a suspect's criminal behaviour in the physical world. However, there is also some incoherence to the level of prerequisites. Not all coercive measures have special prerequisites in respect of cybercrime or the network environment, and not all prerequisites correspond coherently to the invasiveness of each measure. Additionally, as cybercrime becomes progressively more organised, the unavailability of telecommunications interception in cybercrime investigations may come to be seen as more problematic. Already, there have been calls for widening the possibilities for the use of this power in relation to cybercrime offences.[74]

Concerning the eternal dilemma of criminal justice, the balance of efficiency and the rights of the individual, covert coercive measures are the most problematic of law enforcement powers. These measures are highly invasive, and their covert nature means that the targeted individuals have very limited

[73] See the debate relating to the FBI–Apple encryption dispute in the United States of America. Much has been written on this, and the reader will find numerous commentaries, opinions, and statements by legal scholars, journalists, bloggers, technology companies, civil rights advocacy groups, etc., available online. The references cited here will help with a further search: Apple's customer letter (www.apple.com/customer-letter/) and the FBI director's comments (https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter). The case relating to the San Bernardino shooting was eventually dropped after the FBI found a way to unlock an iPhone without help from Apple; see for example the news article by the New York Times (http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html).

[74] Arto Hankilanoja, *Poliisin salainen tiedonhankinta* (Helsinki: Talentum, 2014), p. 107.

possibilities to react or defend themselves while they are subjected to the measures. Therefore, it is not enough that the use of the measures is limited to the investigation of specified offences, and that the decisions are made by a high-ranking official or a court. Additional safeguards are needed, and indeed, are present in Finnish law. In his recently published dissertation on the covert measures and the protection of private life, Tuomas Metsäranta differentiates between conditions of use, minimisation mechanisms, and controlling mechanisms. In this paper, it is not possible to evaluate the various safeguards and their adequacy in detail, but it is worth mentioning that Metsäranta's research suggests the need for a new, independent oversight body.[75]

Concluding remarks

In general, the Finnish legislation on coercive measures does not seem to cause insurmountable problems for the efficiency of criminal investigations. Of course, no legislation is perfect and some legislative adjustments could surely be applied to improve and clarify the situation. On the other hand, Finnish law provides safeguards for the protection of the targeted individual and for minimising the invasion of third parties' rights. Nevertheless, great privacy risks are certainly involved, and there are some problems in the adequacy of these safeguards, especially in relation to covert measures and the supervision of their use.

Although not addressed specifically in this paper, the connections between material criminal law and procedural law should not be ignored. Without going into detail, procedural law should serve the realisation of the material law, and material law should not be impossible to realise. For example, if the elements of an offence cannot be proven because no suitable evidence ever comes to existence, or because such evidence cannot be legally collected, the very value of such a criminal provision is questionable.

However, not all of the problems associated with the collection of evidence in cybercrime investigations are dependent on domestic procedural or material legislation. As hinted earlier in the paper, major impediments are presented by international issues which can be solved only through international cooperation, both legislative and operative. Moreover, even the best legislation on coercive measures is not enough if the investigatory authorities lack the competence, tools, methods, and resources needed to investigate cybercrime and to collect relevant evidence. And of course, in the big picture, the efficiency of *after the fact* investigations of offences is just one of the factors in opposing cybercrime. Crime prevention activity by the police and various preparatory and defensive measures by potential victims can go a long way in reducing the harms of cybercrime.

The rivalry between perpetrators and investigators of cybercrime will continue for the foreseeable future. It will not be beneficial for the progressively more network-dependent societies if the criminals gain an even more substantial lead. Yet, attempts to deal with cybercrime by introducing disproportionate and invasive evidence collection powers might not lead to any better consequences for the majority of law-abiding citizens and Internet users. As always, the efficiency of criminal investigations and the rights of the individual must be kept in balance. While cybercrime, technology, and the world around us continue to evolve, maintaining the balance requires constant adjustments.

Juhana Riekkinen is a Researcher and a Ph.D. (LL.D.) Candidate at the University of Lapland, Faculty of Law. His research focuses on electronic evidence in the Finnish criminal procedure. Currently, he works as a Trainee District Judge in a court training program.

juhana.riekkinen@ulapland.fi

https://lacris.ulapland.fi/fi/persons/juhana-riekkinen(9ce3ca2b-d511-4b2e-b8c4-515d8d074601).html

[75] Tuomas Metsäranta, *Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja* (Turku: University of Turku, 2015), pp. 338–339 (English summary).