Text as accepted for publication by *The Journal of Criminal* Law.

A comparative Analysis of Anglo-Dutch approaches to "cyber policing": checks and balances fit for purpose?

Chrisje Brants, Adam Jackson & Tim J Wilson[1]

Chrisje Brants (corresponding author), Professor of Law, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK **E-mail**: chrisje.brants@northumbria.ac.uk

Adam Jackson, Associate Professor and Deputy Director, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK

Tim J Wilson, Professor of Criminal Justice Policy, Centre for Evidence and Criminal Justice Studies, Northumbria University Law School, Newcastle upon Tyne NE1 8ST, UK

Abstract

This article examines two contrasting approaches to the governance of police investigations for ensuring that cybercrime-policing is lawful and ethical. The Netherlands has a national police force working under the direction of an equally centralised prosecution service according to specific laws on the use of special powers of surveillance, with evidence tested judicially when added incrementally to the case file. Theoretically, the process of adapting to the novel features of cybercrime policing should be much easier than within the much more fragmented policing structure in England and Wales, where unreliable evidence is challengeable only at the trial stage and the laws governing police action are equally fragmented. The Dutch police, however, have not found it easy to adapt concepts of covert policing developed in the 1990's to their on-line investigative activities, despite the existence of comparatively detailed guidance and case law for undercover policing in the "real" world. In the UK, the police seem unsure which requirements and concepts actually apply to their different on-line-investigations. More generally, it is concluded that legal comparisons of the kind undertaken in this article can identify general bottlenecks and barriers to adapting to the cyber environment, but such analysis cannot identify best practices that are readily transferable from one country to another. Legal transplants are a potentially hazardous undertaking because any practices and policies that work successfully will do so because they are necessarily compliant with the underlying systemic legal-cultural factors that make each legal system unique. Indeed, we make no attempt to identify best practices, other than to remark that the centralised nature of Dutch policing seems to afford some advantage, although, for historical and legal-cultural reasons, centralisation is unlikely to be an option for the UK police forces

Key words

cybercrime, police organisation, Dutch prosecution service, disclosure, admissibility

Introduction

[1] With thanks to Wouter Stol for his help on finding information about the Netherlands that we would otherwise have been unable to trace.

In this contribution that is concerned with the response of the criminal justice system to cybercrime, we examine with how different countries (England and Wales and the Netherlands) deal with policing crime on the internet.[2] We do not intend to engage in the debate around the definition(s) of different forms of crime that may be committed with the use of digital devices.[3] Rather, we want to focus on the particular problem of regulating cyber-policing on both the clear and dark web, although we do wish to explain at the outset what we understand by cybercrime.

The Crown Prosecution Service (CPS) in England and Wales recognises two "overarching" areas of cyber-crime:

- cyber-dependent crimes, which can only be committed through the use of online devices and where the devices are both the tool to commit the crime and the target of the crime – e.g. Distributed denial of service (Ddos) attacks; and
- cyber-enabled crimes, traditional crimes which can be increased in scale by using computers.[4]

The approach of the CPS mirrors that of the UK government's National Cyber Security Strategy 2016-21,[5] resulting in a broad definition of cyber criminality encompassing not only *de facto* computer crime but also "traditional" criminality that involves the use of a digital or cyber element in its commission. As Karyda and Mitrou identify:

A cybercrime is an electronic crime that is perpetrated using the Internet, or a crime whose "crime scene" is the Internet. Cybercrimes are not necessarily new crimes; many cases involve rather classic types of crimes where criminals exploit computing power and accessibility to information.[6]

It is this definition of cybercrime that we have adopted for the purposes of this article, although we shall sometimes use synonyms such as "on-line-crime", "internet-crime" or "digital crime". This covers the regulation and/or supervision of the police response to crime on the clear and the dark web, to "new crimes" that can only be committed by digital means and traditional crimes that are "enhanced" by the use of digital devices. There is a considerable body of literature about how and why such criminality poses a new challenge for police and the criminal justice system, and also on whether police and criminal justice institutions are sufficiently resourced and competent to meet these challenges.[7] This article is concerned with whether current procedural and evidential frameworks provide sufficient checks and balances, and with the development of systems, strategies to ensure that the regulation of policing in cyber space is fit for purpose. The question will be answered through analysis of the relevant structures, procedures and policies for policing cybercrime and the digital environment in England and Wales and the Netherlands.

A comparison with the Netherlands could provide some interesting insights. We may expect a number of problems to be the same (indeed, the definition of cybercrime in the Netherlands is practically identical, although not always clearly distinguished from

[2] See Brants, Johnson and Wilson in this issue for the background to this research.
[3] See e.g. D.S. Wall, *Cybercrimes: The transformation of crime in the information age*, (Polity: Cambridge, 2007).
[4] https://www.cps.gov.uk/cyber-online-crime
[5] HM Government, *National Cyber-Security Strategy 2016-2021*, (HM Government: London, 2016) 17.
[6] M. Karyda & L. Mitrou, Internet Forensics: Legal and Technical Issues (2007) *Proceedings of the Second International Workshop on Digital Forensics and Incident Analysis* (Institute of Electrical and Electronics Engineers: New York, 2007) 4.
[7] See also Davies in this issue.

"computer crime"); however, regulatory structures differ significantly. Unlike England and Wales, the Netherlands has one national police force, which should make the development of compatible technological capability easier, and also the consequential adaptation of a common operational practice to engage in cybercrime-policing in a lawful and ethical manner. It also has a longstanding legal culture in which centralised policy and guidance on the use of police powers play an important part in the criminal justice system. Both of these aspects – or rather the lack of them – are cited by British police as hampering the development of efficient online policing.[8] But before we come to a comparison, we must first set out the scale of cybercrime, the structures of cyber-policing and the rules by which cyber-policing is currently governed. We make no pretence at an encyclopaedic overview of all the problems and proposed solutions, or of all the official documents that set out policies and strategies in both countries; the amount alone suggests how important cybercrime has become as a policy issue. Indeed, for the Netherlands many documents are not publicly available.[9]

Cyber-policing: A growing challenge

Cybercrime is a major and developing criminal justice consideration. In 2018, UK and Dutch citizens self-reported broadly similar degrees of awareness of cybercrime risks and direct experience of crimes such as phishing, on-line fraud and hacking, in some instances and especially for awareness, well above the EU 26 average.[10] This is reflected in the significance of cybercrime within crime and security strategies in both countries.

The Crime Survey for England and Wales for the year ending March 2017[11] identified that, of the 3.4 million incidents of fraud experienced by adults that year, over half (57%; 1.9 million incidents) were cyber-related. In addition, adults experienced an estimated 1.8 million incidents of (criminal) computer misuse; around two-thirds (66%; 1.2 million incidents) of these were computer virus-related and around one-third (34%; 0.6 million incidents) were related to unauthorised access to personal information (including hacking). Just how this compares to the Netherlands is not easy to say as Dutch statistics make different distinctions. In any event, in 2018, 8.5% of internet users older than 12 (about 1.2 million people) declared they had been a victim of digital crime in the previous 12 months. The most frequent type of crime was financial, although 1.8% concerned the victims of hacking and more than 2% had experienced personal threats, stalking or sexual victimisation. Just over 1% suffered identity theft or fraud.[12] A recent study by the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) also found that the victim-impact of on-line crimes, be they stalking, bank-fraud or identity theft, is as high as – and usually even higher than – off-line criminality.[13] No wonder then that policy and consultation documents in both countries identify developing strategies to combat cybercrime or cyber-enabled crime as a key

[8] Attempts to address fragmented organisation were noted during empirical research, including Chatham House Rule NPCC organised conferences on 22-25 October 2018 and 19-21 November 2019, and at a research project organised multi-professional workshop held on 12 June 2019 when significant differences in approach between forces were identified as a problem.

[9] However, see for a very detailed, though no longer entirely up to date, paper on the situation in the Netherlands, A.M.G. Smit (2013), *Criminal law on cyber-crime in the Netherlands AIDP Country Report Section 4* < http://www.penal.org/sites/default/files/files/RH-11.pdf > last accessed 7 May 2020.

[10] EC, *Special Eurobarometer 480: Europeans' attitudes towards Internet security* (EC: Brussels, 2019) 25 and 27.

[11] ONS, *The Crime Survey for England and Wales for the year ending March 2017* (ONS: Newport, 2017).

[12] Central Bureau of Statistics *Report 'Digitale veligheid en criminaliteit'* [Digital security and crime]: https://www.thehaguesecuritydelta.com/media/com_hsd/report/249/document/veiligheid-en-criminaliteit.pdf > last accessed 7 May 2020.

[13] NSCR, *Gevolgen cybercrime zeer ingrijpend voor slachtoffers* < https://www.nscr.nl/gevolgen-cybercrime-zeer-ingrijpend-voor-slachtoffers/ > last accessed on 7 May 2020.

priority,[14] while in the Netherlands, cybercrime features large on the research agenda of the Dutch Police Academy.[15]

The growth of cyber-criminality is, per definition, not a national or regional phenomenon. Europol's 2019 Internet Organised Crime Threat Assessment (IOCTA) highlighted the "persistence and tenacity of a number of key threats"[16] in respect of cyber-criminality across the European Union and beyond. The extra-jurisdictional nature of the internet and the ease of global digital communication and data storage often add an international element to investigations, evidence gathering and prosecutions carried out by national criminal justice authorities. At the same time, the increasingly ubiquitous nature of digital devices in society poses significant challenges for law enforcement agencies and the wider criminal justice system, including *inter alia* the amount, complexity and reliability of digital evidence collected and the way in which such evidence is interpreted, stored and disclosed.

Other aspects of cybercrime and "cyber-policing" that compound the difficulties are: the transnational nature of the internet, so that the devices through which crimes are committed may be situated in another country and are therefore not within the usual jurisdictional reach of national law enforcement agencies; the fact that online policing requires certain (new) competences and skills; that it almost inevitably entails a breach of the privacy of the person using the device; and that in the interests of the investigation (and future investigations) it is important that (the nature of) police activity remains hidden, while different countries have different laws governing such undercover policing, making international police co-operation difficult.[17]

While on-line investigation very often implies covert investigation, the regulations and case law governing such policing were mostly drawn up before the advent of cybercrime and the internet, and it maybe unclear as to whether they can be adapted to fit on-line policing. This applies to both the UK and the Netherlands. No wonder then too, that the police are uncertain as to what they can actually do during on-line investigations: do they, for example need authorisation to interfere with a device (possibly in another country), from whom, for which activities and at what point? What are the consequences of failing to obtain authorisation? How to cooperate with law enforcement agencies in other countries and to make sure that evidence they may have obtained there, according to their own rules, is valid

---

[14] See, for example, Home Office, *Cyber Crime Strategy*, (Cm 7842, 2010), HM Government, above, n. 5; DDCMS and the Home Office, *Online Harms White Paper*, (CP 57, 2019). For the Netherlands: most recently Security Agenda 2019-2022, Parliamentary records IIK, r 2018–2019, 28 684, nr. 54; and *Opsporing, vervolging en verstoring van cybercriminaliteit; cybercrime onderzoeksagenda*, the cybercrime research agenda of the WODC (the government's independent crime research centre), part of the wider national research agenda *Cybersecurity beeld Nederland 2018*, produced by the Nationaal Coördinator terrorismebestrijding en veiligheid (NCTV): < https://www.nctv.nl/documenten/publicaties/2018/06/13/cybersecuritybeeld-nederland-2018 > last accessed 7 May 2020.

[15] The research agenda of the Dutch Police Academy comprises eight themes. The first is called "What is coming towards us?" and is about technological developments. The second one is "Police in connection with neighbourhood-web-world". Number four is "State of the art technology and intelligence". In other words: 3 out of 8 themes are directly concerned with the digitization of society. This too is a sign that police capacity (and money) is being assigned to questions in the sphere of digital developments. Next, in the national "Agenda for the development of local police care" the first task for the police is described as "Doing police work in neighbourhood and web". See < https://www.politieacademie.nl/kennisenonderzoek/Onderzoek/onderzoekers/Documents/19193%20190911%20DEF%20Strategische%20onderzoeksagenda%20Boek%20B5%20DIGI.PDF > last accessed 7 May 2020.

[16] Europol, *Internet Organised Crime Threat Assessment* (IOCTA) 2019, (Europol & EC3 (European Cybercrime Centre), The Hague, 2019) 6.

[17] See Davies in this issue, on the problems arising from police international cooperation when procedural safeguards vary significantly between jurisdictions.

in the national courts? Is there sufficient guidance and are there clear policies available? And where can they be found?

Worries about lawfulness and legitimacy by no means form a problem specific to UK or Dutch policing. In the United States, it appears that not only the police but also the courts struggle with such questions, while different courts have given different answers.[18] In the Netherlands too, where many policy documents have highlighted the necessity of developing the potential of digital investigation,[19] police have problems in knowing how to adapt concepts of covert policing developed in the 1990's , to their on-line investigative activities, despite the existence of fairly detailed guidance and case law for undercover policing in the "real" world. They have called for more detailed legislation and instructions to enable them to know what is and what isn't legitimate policing on-line.[20]

The "structure" of cyber policing

Cyber-policing may seem more complicated than its "real-world" counterpart, but it is still policing and, as such, covers the usual aspects of what that concept implies: maintaining law and order and addressing security and safety issues of the population and the state by investigating and bringing criminals to justice; securing (reliable) evidence of crimes; identifying threats, perpetrators and victims; prosecution, deterrence, disruption and prevention; all the while ensuring that such activities do not unduly infringe on individual civil rights and freedoms. These are the goals of police forces in every (democratic) country, but the way they attain them can be very different. It is often said that understanding differences in substantive and procedural laws is essential to international police cooperation, or, put another way, that they hinder effective cooperation and may lead criminals to engage in forum-shopping. Indeed, the foreword of a recent report of the Internet & Jurisdiction Policy Network postulated that; "[h]ow to handle the coexistence of heterogeneous laws on the cross-border internet is one of the greatest policy challenges of the digital 21st century."[21] There is some evidence that police also go on shopping sprees, this time to find the jurisdiction most favourable to certain activities that are forbidden in their own country.[22] However, more important perhaps than knowing what the differences are is to understand the underlying ideology of policing – the generally accepted concept in a given country of what the police are and should be and do – that informs the differences in the laws that govern policing and its organisational structure.

In terms of historical origins, a traditional – and very biased – view of the difference between policing in England and Wales and on the Continent has it, in the words of C.H. Reith that "Gendarmerie police have normally depended for their power on their ability to inspire fear by the tyrannical practices which they are allowed to exercise. In most countries where they function they are regarded by the public without respect or admiration, and with contempt and dislike, but they have usually succeeded in providing an effective solution to

[18] M. R. Shillito, Untangling the 'Dark Web': an emerging technological challenge for the criminal law (2019), *Information & Communications Technology Law*, 28:2: 202-203 and S.D. Brown, 'Hacking for evidence: the risks and rewards of deploying malware in pursuit of justice' (2020) 20 *ERA Forum*:428.
[19] See n.15.
[20] W. Stol & L. Strikwerda, Online vergaren van informatie voor opsporingsonderzoek. Een beknopte evaluatie van voorgestelde wetgeving (2018), *Tijdschrift voor Veiligheid* (17) 1-2: 8-22.
[21] D. Svantesson, *Internet and Jurisdiction: Global Status Report 2019 - Key Findings*, (Internet and Jurisdiction Policy Network: Paris, 2019) 2.
[22] See Davies in this issue, on the problems of police participating in criminal offences, i.e. uploading images of the sexual abuse of children, which is forbidden in most but not all jurisdictions, but is usually a prerequisite of the undercover policing of child abuse sites.

the problem of enforcing laws in spite of their manifest defects".[23] In contrast, British policing is seen as "a model of a democratic and civil police that performs its tasks in strong agreement with the people".[24] Such notions underlie the traditional dichotomy of policing by consent (UK) versus policing by power (the Continent) – the citizen police, of and for the people, versus the police as the long arm of the state. As Fijnaut points out,[25] this is a caricature, based on 19th Century prejudice towards all things French/Napoleonic (and therefore nasty) and equally mythical views of peaceful, democratic England and her citizen police force with its autonomous constabulary and style of community policing. In reality, "the history of the provincial police forces in England […] testifies to less harmony, consensus, and agreement with the people than Reith probably could have believed. The work of C. Steedman, Policing the Victorian Community, is a clear piece of supporting evidence for this view".[26] In any event, particularly in the past decades, British policing has come much closer to its Continental counterpart: partly because of the advent of the CPS and legislation governing (the use of) police powers, partly as a consequence of the harmonizing tendencies of the European Union and the European Convention on Human Rights and Fundamental Freedoms with its case-law of the European Court of Human Rights (ECtHR) and, again, in part due to years of cooperation in Europol and Eurojust.

Nevertheless, historical distinctions still play a part in the differences between policing in England and Wales and the Netherlands. The general organisation of the Dutch police has always been that of an armed state force (Reith's despised "gendarmerie"), which, although regionalised until recently, is now one centralised police force. Its power – and therefore potential for destructiveness – is mitigated by its relative lack of autonomous powers and subordination in criminal matters to the Dutch Prosecution Service and, in the final event as required by the principles of *Rechtstaat*, to the law and oversight by the courts. This means that, as far as the exercise of police powers is concerned, the police may only act, i.e. infringe on citizens' freedoms, if their actions are necessary and proportionate, and specifically authorised by law. The Dutch Police Act, which conveys policing powers to maintain law and order, is regarded as too generally worded. This is also the position of the ECtHR. Wielding powers or using methods that have no basis in law of sufficient specificity (be it written or case law) is unlawful policing.

By contrast, in England and Wales, the autonomous constabulary has evolved into territorial police forces whose chief constables have considerable autonomous power, while the CPS has no formal authority over police activities. As in the USA, the idea of the citizen police is reflected in the notion that the police may do whatever anyone else may do as long as it is not forbidden – a position increasingly limited by legislation governing police investigations such as the Police and Criminal Evidence Act (PACE) 1984, the Criminal Procedure and Investigations Act (CPIA) 1996, the Regulation of Investigatory Powers Act (RIPA) 2000, the Investigatory Powers Act (IPA) 2016, such regulation being required by the principles enunciated by the ECHR. Successive scandals arising out of miscarriages of justice, were needed as a catalyst, [27] however, for even such limited codification of police powers. Such historical cultural differences are relevant to how different criminal justice systems respond to social and economic change, such as the emergence of cybercrime.

---

[23] . H.C. Reith, *The Blind Eye of History* (Faber and Faber: London,.1952).

[24] C. Fijnaut, The police and the public in western Europe: a precarious comparison (1990) 63 *Police Journal* 337-345.

[25] Ibid. 339.

[26] Ibid., where Steedman is referenced as: Steedman, C., *Policing the Victorian Community* (Routledge and Kegan Paul: London, 1984).

[27] C. Walker, 'Miscarriages of Justice in Principle and Practice' in and K. Starmer (eds.), *Miscarriages of Justice: A Review of Justice in Error* (Blackstone Press: London, 1999) 45-52 and 61-62.

Whereas the civil law system of Continental Europe puts its trust in the codification of legal principles and regards the state (and its functionaries) as bound by the ensuing written laws, which renders it slow to be able to respond to change, the preference in common law England, even in relation to fundamental principles, is for the law to be developed by reference to the issues raised in a particular case rather than risk future inflexibility and inappropriateness.[28] This pragmatism has its disadvantages, where flexibility and the means to quickly develop appropriate rules also mean uncertainty as to what the law actually says and its proper application.

Policing the digital world, and in particular the dark web, often requires the use of covert methods that infringe on fundamental rights (privacy, freedom of expression). In the Netherlands where all police action requires a specific basis in law, undercover policing is strictly regulated in detail in the Code of Criminal Procedure (CCP) and is, moreover, governed by (policy) directives from the Prosecution Service; the problem for Dutch police is to know what these regulations mean for cyber-policing. This is also true of England and Wales, where the investigative process is underpinned by a series of authorisations necessary for the deployment of intrusive powers for example, directed surveillance, search of premises and seizure of evidence and so called "equipment interference". Police power to exercise such intrusive powers may be derived from a range of statutory authorities (PACE 1984, RIPA 2000, IPA 2016 etc.) depending on the particular power being exercised. Here, however, detailed guidance seems less available, and the uncertainty seems to be which rules are activated by which activity. This is compounded by the lack of centralised organisation characteristic of UK policing, which like the US model consist of 'highly diversified tapestries of local, regional and national with complex inter-relationships'.[29]

Policing Cybercrime: organisation in England and Wales

Policing in England and Wales has a traditionally devolved structure with 43 territorial police forces in England and Wales[30], each covering a specified geographical area[31]. The National Police Chiefs' Council (NPCC)[32] brings together senior officers from all police force areas and is responsible for coordination and reform of policing at a national level. Overall responsibility for policing policy rests with the Home Office; however, responsibility for responding to aspects of cybercrime will be shared with other departments, on-line abuse for example also falling within the remit of the Department for Digital, Culture, Media and Sport.[33]

The National Crime Agency[34] (NCA) was formed in 2013 as a national law enforcement agency responsible for coordinating the policing of organised crime across the UK.[35] The NCA is not a separate police force but instead is a non-ministerial government department accountable to the Home Secretary who is responsible for directing the strategic priorities of the NCA[36]. Although the NCA has a power to direct police operations (with the Home Secretary's consent) it tends to work collaboratively with territorial police forces and other agencies under a series of voluntary arrangements to coordinate responses to the threat of

[28] See e.g., Lord Bingham, *The Rule of Law* (Allen Lane: London, 2010) 7-8.
[29] B. Bowling, R. Reiner and J. Sheptycki, *The Politics of the Police*, 5th Edn (OUP: Oxford, 2019) 246.
[30] < https://www.police.uk/forces/> accessed 7 May 2020; Police Act 1996 (as amended), Schedule 1.
[31] In addition to the territorial police forces there are 4 'special' police forces; the British Transport Police, the Civil Nuclear Constabulary, the Ministry of Defence Police and The Port of Dover Police.
[32] < http://www.npcc.police.uk/Home.aspx > accessed 7 May 2020.
[33] See e.g. DDCMS and the Home Office, above n.14.
[34] .< http://www.nationalcrimeagency.gov.uk/ > accessed 7 May 2020.
[35] Crime and Courts Act 2013, c.22, s.1.
[36] Ibid. s.3.

organised crime. The NCA also houses the National Cyber Crime Unit[37], which is responsible for leading the UK's response to cyber-crime threats.

The UK's National Cyber Security Centre (NCSC)[38] was launched in October 2016 as "a single point of contact for SMEs, larger organisations, government agencies, the general public and departments".[39] The NCSC was established under the UK Government's National Cyber Security Strategy 2016 - 2021[40] "to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilities (sic) and providing leadership on key national cyber security issues."[41] Whilst the NCSC's remit is broader than law enforcement, it is required to "work collaboratively with other law enforcement, defence, the UK's intelligence and security agencies and international partners."[42]

At a regional level, thirteen Regional Organised Crime Units (ROCUs) provide "a range of specialist policing capabilities"[43] to territorial police forces. These ROCUs work in partnership with the NCA and NCSC to support and coordinate investigations into organised crime, including cybercrime. Whilst each territorial force sets its own strategic policing priorities in collaboration with their local Policing and Crime Commissioner, the ROCUs provide a conduit between locally led investigations and NCA supported operations at a regional, national or international level.

Policing Cybercrime in The Netherlands

Since January 1st 2013, the Dutch police have been (re)organised into one national police force with, at the national level, one police management team and one chief of police, accountable to the minister of Security and Justice (who is, in turn, accountable to Parliament). This national force is divided into ten regional units, each with their own unit management and dealing with high impact crimes, the most serious cases going to units at the national level. Regional units are subdivided into districts (again subdivided into basic teams which deal with relatively simple, frequently occurring crimes). There are 43 districts in total and 168 basic teams. There is also one central, national unit designed for transregional and specialist policing, with various services, of which the National Investigation Service is engaged in the fight against serious and organised crime and other serious crimes such as child pornography and "high tech crime".[44]

The Team High Tech Crime (NTHTC) plays an important part in cyber-policing at the national level and is charged with investigating the most difficult cyber-cases (i.e. internationally organised or politically sensitive cybercrime).[45] But it is not the only unit involved, as digital crime is also dealt with at the regional and local level.[46] As of 2016-2017, the police were engaged in setting up "cybercrime teams" at a regional level, who also support colleagues at the local level in need of extra, specialised and/or technical knowledge. Some of the regional units have so-called "digital platforms" that function as front-line digital support for investigative teams and officers. The organisational structure differs per regional unit and is still very much a matter of ongoing development.

---

[37] < https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime > accessed 7 May 2020.
[38] < https://www.ncsc.gov.uk/ > last accessed 7 May 2020.
[39] < https://www.ncsc.gov.uk/section/about-ncsc/what-we-do > last accessed 2 January 2020.
[40] HM Government, above n. 5.
[41] Ibid. para 1.9.
[42] < https://www.ncsc.gov.uk/section/about-ncsc/what-we-do > last accessed 2nd January 2020.
[43] < https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus > last accessed 2nd January 2020.
[44] See W. Stol and L. Strikwerda, *Law Enforcement in Digital Society*: (Eleven International Publishing, The Hague, 2019) 237-239, for a more elaborate description and schematic overview.
[45] See Davies in this issue for more on the role of the NTHTC.
[46] Again see Stol and Strikwerda, above n. 44 at 247-256, for detailed explanation.

There is however a tendency to specifically prioritise and organise the fight against certain forms of cybercrime. In 2011, the Programme for Improving the Combatting of Child Pornography[47] resulted in a team for tackling child pornography and child sex tourism at the national level and through ten regional teams, with centralised prioritisation and allocation of cases. If necessary, the NTHTC can provide technical support, while a "Dark web-team" deals with investigations on the dark web. There is also an Electronic Crime Task Force (ECTF), in which the police, the Prosecution Service and the banks collaborate to prepare online fraud cases before handing them over to a regional unit. The National Internet Fraud Hotline receives reports from citizens about online fraud, assesses them, prepares the investigation and again hands over to a regional team. Finally, the National programme to Intensify Tackling Cybercrime supports the police in implementing the Ministry of Security and Justice's 2015-2018 Security Agenda in relation to cybercrime prevention.

According to Stol and Strikwerda, the organisation of cybercrime-policing in the Netherlands is still in a transitional phase, with current organisational measures merely temporary. These authors foresee that the idea of organisation at three levels (national, regional, local) may disappear in the face of centralisation and thematic organisation (the current backbone of police work, neighbourhood policing, becoming simply one more theme among many, including child pornography and identity fraud).[48] Increasingly too, centralisation is required for international cooperation, with other police forces and with Europol and Interpol; at present, this is the remit of the NTHTC. At the same time, Stol and Strikwerda predict that (the fight against) cybercrime will cease to be a specialism, and that now "specialised" units will once again take their place in the normal fight against crime. All of which is not to say that specialised technical knowledge will no longer be required, or that policing cyberspace does not bring extra complications.

The challenges of implementing coherent cyber policing polices: setting strategic priorities

As discussed above, while many types of cybercrime (particularly in respect of cyber-enabled crime) are not new per se, the technological, transnational and extra jurisdictional nature of cybercrime makes it difficult to fit into traditional policing paradigms. This is compounded by the subsumption of cyber-policing within a more general cyber-security narrative. Whilst Lavorgna and Sergi identify that "it is not surprising that cybercrime is receiving increasing attention… at the policy level"[49] there appear to be challenges in setting specific strategic priorities and policies for policing in this area in the UK, particularly at the local or regional level.

The basis of UK cybercrime policy is outlined in the 2010 Home Office Cyber Crime Strategy[50] (the 2010 strategy) and latterly the UK Government's National Cyber Security Strategy 2016 – 2021 (the 2016 strategy).[51] The five overarching aims of the 2010 strategy are to:

- Coordinate activity across Government to tackle crime and address security on the internet in line with the strategic objectives laid out in the UK Cyber Security Strategy;

[47] Parliamentary Papers, IIK 2010/11, 32500 VI, no. 102.
[48] Stol and Strikwerda, above n. 44 at 259.
[49] A. Lavorgna and A. Sergi, Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom, (2016) 10 *International Journal of Cyber Criminology* 175.
[50] Home Office, above n.14.
[51] HM Government, above n. 5.

- reduce the direct harms by making the internet a hostile environment for financial criminals and child sexual predators, and ensuring that they are unable to operate effectively through work to disrupt crime and prosecute offenders;
- raise public confidence in the safety and security of the internet, not only through tackling crime and abuse, but through the provision of accurate and easy-to-understand information to the public on the threats;
- support industry leadership to tackle cybercrime, and work with industry to consider how products and online services can be made safer and security products easy to use; [and to]
- work with international partners to tackle the problem collectively.[52]

It is noteworthy that the 2010 strategy situates cybercrime within its broader cyber-security context. This appears to be consistent with what Lavorna and Sergi consider to be "the emergence of a non-evidence-based "cyber-organised crime" rhetoric"[53]. This becomes even more explicit when considered alongside the 2016 strategy. The 2016 strategy deals with cybercrime as one of a number of potential cyber security threats, largely in the context of threats from organised crime groups (OCGs) and foreign actors, predicated on the wider threat to national security and infrastructure.[54]

The UK's 2016 strategy does recognise that "[w]hilst OCGs may pose a significant threat to our collective prosperity and security, equally of concern is the continuing threat from acts of less sophisticated but widespread cybercrimes carried out against individuals or smaller organisations.[55] The 2016 strategy further considers that "[t]he primary duty of the Government is to defend the country from attacks by other states, to protect citizens and the economy from harm, and to set the domestic and international framework to protect our interests, safeguard fundamental rights, and bring criminals to justice."[56]

In the UK at least, it appears that a key challenge in cyber policing policy and the setting of strategic priorities in this area derives in part from the structure of policing in England and Wales. Outside of the larger, more heavily resourced investigations into cyber-crime, typically prioritised because of the broader cyber security threat that they pose and typically coordinated by the NCA, it is less clear how the police in England and Wales tackle the more general threat of cybercrime in a coordinated way. Bodies such as Action Fraud[57] provide a role in identifying the scope of the problem faced and provide a central point of contact for reporting of these issues but in practice do little more than record instances of online fraud and coordinate the dissemination of reports to relevant police forces. At a local level, and in the context of finite resources, individual territorial police forces to a large extent set their own strategic priorities. At the very least this makes it difficult to identify a coordinated approach to the growing general threat of cyber criminality beyond the larger, more coordinated operations against perceived threats to national security or infrastructure or which are part of efforts to tackle more sophisticated and organised criminal offending.

In the Netherlands too, government policy (as set out in the government coalition agreement of 2012)[58] recognises "increasing threats and vulnerabilities in the field of

---

[52] Ibid at at17.
[53] A. Lavorgna and A. Sergi, above n. 49 at 171.
[54]. HM Government, above n.5.
[55] Ibid. at para 3.6.
[56] Ibid at para 4.9.
[57] < https://www.actionfraud.police.uk/ > ;last accessed 5 April 2020.
[58] < https://www.europa-nu.nl/9353000/1/j4nvih7l3kb91rw_j9vvj9idsj04xr6/vj46ifemvrmj/f=/regeerakkoord_vvd_pvda_2012.pdf > last accessed 7 May 2020.

cybersecurity". These are to be met through joining forces with all stakeholders, reinforcing investigative capacity and adapting legal instruments to changed circumstances". At the same time, one of the important recent Dutch policy documents was released by the National Coordinator for Combatting Terrorism and Security, pointing here too to a wider security approach. However, the traditional role of the heads of the prosecution service in implementing criminal justice policy and directing prosecutors (and in their wake the police) by means of binding directives perhaps makes the development of coherent policing policies easier in the Netherlands, can cut through political rhetoric and establish cybercrime as a matter of "normal" policing.

The Netherlands: supervision of police action and legal requirements

Most readers of this article will be unfamiliar with the governance of Dutch policing and how this is directly derived from the nature of criminal justice in the Netherlands. The same considerations apply to England and Wales where, for example, the emphasis on disclosure and admissibility of evidence that will be considered in the next section, reflects essential fair trial safeguards arising directly out of the requirement of equality of arms in the adversarial style of procedure; there, the trial phase is paramount and provides the only arena in which the case, including police activity and the manner of evidence collection and its reliability, can be (con)tested in adversarial argument. This also means that, if a case is not prosecuted and thereby disclosure requirements set in motion (for example, if the goal of police activity is simply to disrupt the activities of the offender), there will be very little regulated scrutiny of police action. By contrast, the continental-style of policing and inquisitorial procedure in the Netherlands, with its emphasis on pre-trial investigation and the importance of hierarchical oversight to ensure legitimate policing in accordance with the law, requires very different safeguards.[59] The most important could be said to be the role of the prosecutor and the court in scrutinising police investigative activity as to whether it conforms to legal requirements. These are to be found in the Code of Criminal Procedure (CCP) and, given that legislation can be unwieldy in that it may take a long time to amend to fit changing circumstances, in directives from the heads of the prosecution service that clarify and elaborate on the legal provisions. Such directives have the status of quasi law, are public and binding on prosecutors and police, and may be relied upon as a defence in court. Traditionally they form an important aspect of Dutch criminal justice,[60] and also play a role in cyber-policing.

The Explanatory Memorandum to the new Computer Crime Act III (p. 16 and following) refers explicitly to the Prosecution Directive on police powers of investigation[61] which in its turn gives detailed instructions on how to use the powers set out in the Act on Special Police Powers (*Wet Bijzondere opsporingsbevoegdheden*) and which is contained in Book 1 Title IVA CCP. The regulation of these special powers was the direct result of the police exceeding their authority in the 1990's with regard to the policing of organised crime by using covert methods of investigation not regulated by law, article 3 of the Police Act, which confers general powers, being regarded as too non-specific. The resulting scandal is indicative of how deeply engrained in the Netherlands is the notion that the police must only

[59] See C.H. Brants, 'Comparing criminal process as part of legal culture', in *Comparative Criminal Justice and Globalisation* (ed. D. Nelken), (Ashgate: Aldershot, 2011): 49-68.

[60] See on the importance of such directives for criminal justice policy and the setting of proecution and police priorities: E Blankenburg, Beleid – a very Dutch legal term (1999) 30 *Journal of legal pluralism and unofficial law* 65-74.

[61] Aanwijzing opsporingsbevoegdheden *(2014A009)*, ch. 2, 3 < https://beleidsregels.om.nl/opsporing-politie/aanwijzing > last accessed 7 May 2020.

use powers conferred by law and must do so under guidance of the public prosecutor. Acting partly in coordination with the American Drug Enforcement Agency (DEA) as part of the latter's "war on drugs", some regional Dutch forces engaged in undercover policing using methods such as controlled delivery and participating agents that were perfectly normal and legal in the USA but, at the time, had no basis in Dutch law. Some, though not all, prosecutors were unaware of what was going on and in some cases the police used the money obtained through participation and controlled delivery to buy supplies for their own forces. When the scandal broke in the media it was framed as the police being "out of control." This was followed by a parliamentary inquiry (a particularly thorough and public way of investigating public scandal in the Netherlands). The result was a large body of legislation that details what the police can do in undercover work and binds them to seek authorisation from the prosecutor or judge of instruction and to scrupulously record whatever they have done in the course of a covert investigation.[62]

As we have seen, much cyber-policing is covert policing (and often also concerns organised crime) and the Dutch government obviously regard these laws and directives, which are at least 15 years old, as adaptable to the policing of cybercrime. Interestingly, although the Computer Crime Act III with its explicit reference to the Directive on Special Powers entered into force in March 2019, as yet the Prosecution Service has not updated that directive or produced new instructions on how to translate it from the real world to the world of cyberspace; notwithstanding that lack of training for working in a digital environment and lack of knowledge regarding the ins and outs of cyber-policing are cited as two distinct problems for the Dutch police.[63] Such guidance as does exist has usually not taken the form of official directives and is, moreover, not publicly available, which, given the status of policy directives as quasi-law, is unusual. These include "*Half Uur Internetbevraging*" (HUIB) ["Half an hour on the Internet"] which is a document that shows police officers how to systematically and efficiently (no more than half an hour) collect information from the internet. And a document that shows police officers what legislation can or must be used (i.e. which police powers) for what kind of internet search.

The Explanatory Memorandum to the Computer Crime Act III attempts to rectify this lack of official guidance, by setting out how some existing special powers are to be used in cyber-policing. They have in common that, as soon as the infringement of civil rights is at stake, their use requires authorisation from either the Prosecutor or the judge of instruction (investigating magistrate). The rule of thumb is proportionality and necessity: suspicion of a (very) serious crime, while the more serious the infringement, the greater the need for authorisation and the higher and more independent the authorising authority (the judge of instruction being a member of the independent judiciary, while the prosecutor may often be either close to or involved in the investigation). In the case of covert surveillance, for example, no authorisation from the prosecutor is required unless such surveillance entails entering premises (not being a home) and/or becomes systematic, by which is meant an attempt to obtain a complete picture of a person's life.

The Computer Crime Act III introduces what it calls the power to investigate in and interfere with an "automated device" (by which we should understand hacking a computer, smartphone, indeed anything with a digital processor). It explains that the possible infringement of privacy that this could imply, in combination with systematic surveillance (total examination of the content of said device or placing police malware such as a crawler),

---

[62] See *Parlementaire enquête opsporingsmethoden, IRT (1994-1996)* < https://www.parlement.com/id/vh8lnhrpmxw6/parlementaire_enquete_opsporingsmethoden > last accessed 7 May 2020..

[63] W. Stol, R. Leukfeldt and H. Klap, 'Policing a Digitized Society' in: *Cybercrime and the Police* in W.P. Stol and J. Jansen (eds.), (Eleven Publishing: The Hague, 2013).

constitutes such an infringement of individual privacy rights that police need to seek an order from the prosecutor *and* authorisation by the judge of instruction. However, despite detailed explanations, complete with examples, the Explanatory Memorandum does not, indeed cannot, cover all eventualities. Meanwhile, the police themselves have produced several "good practice guides", or farmed the production out to academic research groups. In the final event, it will be up to the Prosecution Service to provide clear guidance. As yet, the only new prosecution directives on cybercrime concern the penalties that the prosecutor should ask for in court for different types of computer crimes[64] and another novum of the Computer Crime Act III, which relinquishes territoriality as a criterion for determining jurisdiction and introduces the power to investigate and interfere with a device regardless of the state where it may be physically found.

The Explanatory Memorandum contains a lengthy justification for this possible infringement of another state's sovereignty, while the concomitant directive explains in detail what action the police and prosecutor should take if they wish to hack a computer, server, smartphone etc. of which the location is unknown or is in a state other than the Netherlands.[65] It also specifically instructs them to follow the usual route to obtain assistance from the authorities in the other country whenever time allows, or to inform that country later.[66] Similar provisions can be found in the United Kingdom in the Investigatory Powers Act 2016 and in legislation passed in the United States of America where the Clarifying the Lawful Use of Data (CLOUD) Act[67] allows for the interception and disclosure of electronic communications in specified circumstances, but regardless of jurisdictional niceties or the usual recourse to international assistance in criminal matters.

In the Netherlands, prosecutorial and judicial oversight of the police is thought to ensure that special powers will be used lawfully, which means that any illegality should be discovered in advance by the prosecution, the defence or the court. Disclosure of evidence does not exist in the same way as in England and Wales and, indeed, is theoretically less important as a safeguard. Nevertheless, as will be considered in greater detail in the next section, defence and court must be aware of what has taken place during the investigation. Because of the paramount importance of pre-trial procedure in Dutch criminal process and the investigative role of the inquisitorial court, there is much less emphasis than in an adversarial system on adversarial debate or the equality of arms and disclosure regime that is meant to guarantee such debate. In normal, i.e. non-digital, circumstances in the Netherlands, procedural requirements dictate the existence of an extensive dossier in which all police activity, all methods used, handling and storage of evidence and warrants and authorisation obtained must be noted, and that forms the basis for the prosecution dossier. This can then be scrutinised by the defence before and by the court during trial, when the judges will have the full dossier to hand when preparing for and examining the case.

However, access to the dossier, which must be through a request to the prosecutor, may be denied the defence "for reasons pertaining to the investigation", such as secrecy with regard to police methods used etc. The defence do have an absolute right to access the dossier from the moment a summons to appear in court is issued. Although defence counsel play a less important part in inquisitorial than in adversarial proceedings, access to the dossier is crucial, and not only because Art. 6 ECHR regards it as part of the requirements of a fair trial (the right to know the evidence and to be able to contest it). Access to the dossier gives Dutch defence counsel an opportunity to point to gaps in the information it contains, to point the

---

[64] *Richtlijn voor strafvordering cybercrime* (2018R001), https://beleidsregels.om.nl/index/richtlijn-8

[65] *Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126NBA SV*, < https://beleidsregels.om.nl/opsporing-politie/aanwijzing-0/ > accessed 7 May 2020.

[66] See Davies in this issue on the details of this police power to hack across borders.

[67] H.R.4943, 115th Congress (2017-2018).

prosecutor to alternative avenues of investigation, to request further investigation by the judge of instruction and to challenge the legality of the way the evidence was obtained.

While there are significant gaps in and questions about the Dutch approach to creating a legal regime that is fit for the purpose of regulating the policing of cybercrime, the criminal justice system and political expectations about how it should work, are geared to respond to criminological changes in a unified and rights compliant manner. In England, as will be seen in the next section, the problems of a fragmented policing system are compounded by the generally slow, possibly reluctant, and more fragmented approach to modernising the law.

England and Wales: supervision of police action

Except for some specialists, it is often difficult to be confident of knowing the current English procedural law regulating the conduct of investigations. In contrast to a Dutch colleague, an English police officer cannot expect to be able to check the law easily in a single current text concerning criminal procedure or obtain guidance from easily referenced memoranda or directives. As indicated in the previous section, while this may not have always been fully achieved in the Netherlands, the cultural expectation is that it should be fully achievable. In England the default expectation among police officers observed in our research appears to be that the law and how it should be applied to cybercrime policing will be obscure or even threatening.[68] This stems from several causes.

The fragmented policing structure with significant disparities in resources and influence in England has already been noted and is clearly important. Other factors also contribute to this situation and are considered in this section: (i) the frequently piecemeal legal development via case law and (ii) the need to identify current statutory law by tracing a series of interlocked amendments made over several years in compendium type criminal justice statutes and, perhaps more controversially, (iii) the greater distance (in terms of the time taken and comprehensiveness of the response) between English law and supra-national fundamental rights jurisprudence. These issues are daily diet for both legal academics, judges and other practising lawyers who have been trained to understand how English law develops and how to apply it accurately. Even in the highly codified Dutch system, some questions of admissibility are left to judicial discretion, but some thought needs to be spared for the impact of legal complexity and uncertainty in England and Wales on investigators already struggling to cope with the volumes, complexities and novel ethical problems of cybercrime.[69]

This is an extensive and complicated subject, and here we can only attempt provide a brief summary through four examples that bring out comparisons and similarities of approach between the Netherlands and England and see some advantage in being able to respond to technological challenges, noting the extent of convergence of legal thinking across jurisdictions[70], if not always in terms of the solution found then at least with some commonality in the underlying principles applicable to problem resolution:

- Data protection in criminal investigations.
- Disclosure of evidence.
- The judicial regulation of the admissibility of evidence during a trial.

[68]Noted during empirical research, including Chatham House Rule NPCC organised conferences on 22-25 October 2018 and 19-21 November 2019, and at a research project organised multi-professional workshop held on 12 June 2019.

[64] The overall impact of cybercrime and rising volumes of digital evidence in traditional offences is acknowledged by Europol as 'a threat to [police] capability to investigate such crimes and identify victims', see: Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (Europol: The Hague, 2018) 31. As to ethical problems, see Davies in this issue on the question of whether police officers, acting as covert participating agents, should be allowed to commit crimes in order to safeguard their cover.

[70] For references to the differing perspectives on the 'convergence thesis' see P. Roberts and A. Zuckerman, *Criminal Evidence*, 2nd edn (Oxford University Press: Oxford, 2010) n. 61 56.

- Centralised quasi-judicial supervision and judicially guided inspections of communication interception, surveillance and equipment inference ('hacking').

It is important to bear in mind that, as will be seen below, sometimes the impact of the solution to one problem in the decentralised English criminal justice system and piecemeal nature of legal development may have important consequences for the ability to resolve other problems.

a) Data protection

Data protection law, partly because it is relatively new, and also because of its commercial importance, is a self-contained and clear area of legal regulation applicable to cybercrime policing. It provides, for example, rules governing the acquisition, use and retention of data relating to persons of interest and victims. In the Netherlands – irrespective of whether it originates in EU law/CJEU jurisprudence or is derived from ECHR/ECtHR – Dutch courts and the data protection authority must apply it directly and it will take precedence over national laws.[71] Post-Brexit in England and Wales, data protection law may come to consist of EU law in force at the time of departure[72] and an evolving system of ECHR law developed by ECtHR and applied indirectly through domestic legislation, especially the Human Rights Act 1998, and case law. [73] There will be strong commercial and security self-interests that might discourage the emergence of differences over data protection between English and EU law. That would mean that, just as issues are currently well understood and detailed official or private guidance is readily accessible for police officers, it is unlikely to cause difficulties in the future for the police in England, at least in the short and medium term.

b) Disclosure

In English and Welsh criminal proceedings a failure to disclose potentially exculpatory evidence to defence lawyers engages Art 6. ECHR. This is not an abstract principle. A former Director of Public Prosecutions admitted to Parliament that some people had been wrongly imprisoned because of such failures in the procedural safeguards intended to ensure that unreliable evidence can be exposed as such and contested during the trial.[74] Disclosure problems are not new (they were highlighted in six reports between 2011 and 2017), nor confined to technological or scientific evidence.[75] The widespread ownership and use of digital devices, "the explosion of digital media" often outside cybercrime investigations, however, has transformed the scale of the problem.[76] It has been is estimated that an average of 35,000 pages of data can be downloaded from every single mobile device examined by police forces,[77] that are also trying to cope with ever increasing volumes of cybercrime.

---

[71] I. Peçi, 'The Netherlands' in K. Ligeti (ed.) *Towards a Prosecutor For the European Union* (Hart: Oxford, 2013) 96; J. Gerards and J. Fleuren, 'The Netherlands' in (eds.) J Gerards and J Fleuren, *Implementation of the European Convention on Human Rights and of the judgments of the ECtHR in national case law* (Intersentia; Cambridge, 2014) 220-223.

[72] Initial post-Brexit guidance to criminal justice organisations (at the time of writing) is that except for minor technical amendments data protection law has not changed and Brexit did not affect day-to-day domestic processing. Also international exchanges with EU member states will not change if an 'adequacy decision 'is in place, see: ICO, *Data Protection and Brexit Law enforcement processing: Five steps to take* (ICO: Warrington, 2019).

[73] R.Masterman, 'The United Kingdom', in (eds.) J Gerards and J Fleuren, *Implementation of the European Convention on Human Rights and of the judgments of the ECtHR in national case law* (Intersentia; Cambridge, 2014) 301-302 and 306-318.

[74] Justice Committee, *Disclosure of evidence in criminal cases* (HC 2017–19 859) para 1.

[75] Ibid. para 22.

[76] David Kirk, How do you solve a problem like disclosure? (2013) 77 *J. Crim. L.* 277.

[77] Justice Committee, above n. 74 para 56.

Prosecution and defence access - particularly during sexual offence investigations - to intimate aspects of offenders' and victims' lives preserved on social media, has also given political and public prominence to a problem that hitherto was the preserve of legal and police experts.

In *R v Malook*[78] the England and Wales Court of Appeal held that the duty to record applies to not only material evidence seized by the police during an investigation, but equally to "documentation produced by the police in the course of investigations in contradistinction to pre-existing material seized by a police force." The court emphasised that "Proper record keeping in an investigation is essential to the integrity of an investigation, to public confidence in police investigations and the proper administration of justice.[79] Responsibility for compliance with the law on disclosure[80] is shared by the investigators (usually the relevant police force), who are responsible for logging the material which is obtained or generated by the investigation, and the CPS which is responsible for determining whether the evidence should be disclosed.

The CPS have published *Guidelines on Communications Evidence*[81] and subsequently guidance on what constitutes reasonable lines of enquiry[82] primarily in response to the failures in disclosure in serious sexual offence cases[83]. Both sets of guidance have to be read in conjunction with the Attorney General's Guidelines on Disclosure,[84] but it is difficult to see how these supplementary guidelines - even if there are no difficulties in dealing with three separate sources of advice - can have a significant impact without a consequent increase in resource for disclosure practices and, perhaps more significantly, consideration of the fitness for purpose of such a self-regulatory regime for disclosure compliance created before the proliferation of online investigations and digital evidence.

In theory at least, the digital and cybercrime volume pressures faced by investigators in the Netherlands should not be so intense because the defence can seek to intervene earlier and significantly in the pre–trial proceedings. Once a suspect has been formally identified, the defence is entitled to see evidence as it is gathered ("added to the file" that will contain all the evidence on which the judicial determination will be based)[85] and can request that additional matters are investigated.[86] As outlined above, neither right is absolute. Access to the file can be restricted temporarily and additional investigations require judicial authorisation. A more pro-active role for the defence on something like the Dutch model might reduce the digital disclosure burden for the police as well as the risk of miscarriages of justice arising from disclosure failures. This however would be very difficult to adapt to an adversarial system where truth-finding depends on the autonomy of equal parties engaging in adversarial debate at trial. Moreover, in practice, Dutch defence lawyers complain that they do not see evidence in time because of how the police and prosecution control the flow of information. This has not, however, given rise to similar scandals that rocked confidence in the English and Welsh criminal justice system in 2018-19,[87] although there has been at least

[78] *R v Malook* [2011] EWCA Crim 254.
[79] Ibid at [35].
[80] Criminal Procedure and Investigations Act (CPIA) 1996.
[81] < https://www.cps.gov.uk/legal-guidance/disclosure-guidelines-communications-evidence, (published 26 January 2018) > last accessed 6 March 2020.
[82] < https://www.cps.gov.uk/legal-guidance/disclosure-guide-reasonable-lines-enquiry-and-communications-evidence > (published 24 July 2018) last accessed 06/03/2020.
[83] Ibid. n. 88.
[84] Attorney General, *Attorney General's Guidelines on Disclosure*, 2013.
[85] I. Peçi, above n.71 at 96; J. Gerards and J. Fleuren, above n.71 at 220-223.
[86] M. C. Van Wijk, *Cross-border evidence gathering* (Eleven Publishing: The Hague, 2017) 137.
[87] Justice Committee, above n.74 at paras 85-86.

one major miscarriage of justice where the prosecution withheld evidence from both defence and court.[88]

If special investigating powers have been used in the Netherlands, a separate dossier outlining these and containing the relevant documents, prosecution orders and judicial authorisations may be presented. It should be remembered that the primary importance here is not disclosure to the defence in order to make equality of adversarial argument possible, but information for the court who must judge whether the investigation has taken place in accordance with the law and whether the evidence meets the requirements of quality, reliability and legality. And it is for the inquisitorial judge to clarify any doubts, if necessary prompted by the defence. Because the defence is dependent on the content of the dossier to raise matters pre-trial with the prosecution or judge of instruction, or at trial with the court, and because there is no total clarity about what documents the dossier should contain – other than those that are "relevant", the district court of Amsterdam ruled that such a "shadow dossier" is "part of the documents of the case and must be presented as soon as the interests of the investigation allow, and not only if it contains evidence – whether incriminating or disculpatory."[89] We may presume that these rules also apply to cyber-policing; the Explanatory Memorandum to Computer Act III specifically states that all activities must be recorded ("logged") with an eye to scrutiny of the investigation.[90] Where police methods or the identity of investigating officers must be protected, it is possible to have the latter testify anonymously and if necessary before the judge of instruction in a procedure separate from the trial, where the defence may also ask questions (though not if these would reveal the identity of the witness, while other questions may be disallowed).

This corresponds to the important exception to disclosure in England although there are major differences, one being that the protection of witnesses continues during the trial phase in the Netherlands, where the transcript of the examination by the judge of instruction is available to the trial court (and the defence) and is regarded as evidence, although the witness may not be present in person to answer questions.[91] The disclosure of sensitive material in England[92] may be withheld on public interest grounds by virtue of a Public Interest Immunity (PII) application. In *R v H*[93] Lord Bingham summarised the operation of PII in the following terms: Circumstances may arise in which material held by the prosecution and tending to undermine the prosecution or assist the defence cannot be disclosed to the defence, fully or even at all, without the risk of serious prejudice to an important public interest. The public interest most regularly engaged is that in the effective investigation and prosecution of serious crime, which may involve resort to informers and under-cover agents, or the use of scientific or operational techniques (such as surveillance) which cannot be disclosed without exposing individuals to the risk of personal injury or jeopardising the success of future operations. In such circumstances some derogation from

[88] The so-called "Schiedam Park case". See on this and other miscarriages in the Netherlands, C. Brants, 'Wrongful Convictions and Inquisitorial Process: The Case of the Netherlands' (2012) 80 *University of Cincinnati. Law Review* 1071.
[89] Rechtbank Amsterdam, 19 oktober 2009, NbSr 2009, 372.
[90] *Wet Computercriminaliteit III*, Parliamentary Records IIe Kamer, 2-15-2016, 34 372, no.3, 31.
[91] The protection of (the identity of) a witness is a complicated matter in the Netherlands and subject to specific rules in the CCP. Some witnesses may appear in court using a number and in disguise; others may simply be heard by the judge of instruction. See W. Dreissen and O. Nauta, *Anonimiteit in het strafproces. De praktijk van de regeling beperkt anonieme getuige en de regeling bedreigd anonieme getuige in het strafproces*, WODC report (DSP-groep: Amsterdam, 2012).
[92] Revised Code of Practice to the CPIA 1996 (s.23(1)), para 6.14, "Any material which is believed to be sensitive either must be listed on a schedule of sensitive material or, in exceptional circumstances where its existence is so sensitive that it cannot be listed, it should be revealed to the prosecutor separately.".
[93] *R v H* [2004] UKHL 4.

the golden rule of full disclosure may be justified but such derogation must always be the minimum derogation necessary to protect the public interest in question and must never imperil the overall fairness of the trial.[94]

c) Admissibility of evidence at trial

In England and Wales, all relevant evidence is prima facie admissible.[95] This includes evidence which has been unlawfully or improperly obtained,[96]although such evidence is subject to possible exclusion on the grounds of unfairness. At common law "[a] trial judge in a criminal trial has always had discretion to refuse to admit evidence if in his opinion its prejudicial effect outweighs its probative value"[97], this discretion subsequently took a statutory form in PACE:[98] In any proceedings the court may refuse to allow evidence on which the prosecution proposes to rely to be given if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.[99] Case law[100] has excluded evidence obtained in consequence of "significant and substantial"[101] breaches of PACE and PACE Code of Practice C[102].

Given what we have said about the principles of policing, it should come as no surprise that in the Netherlands intrusive police investigation is a primary concern, addressed through the detailed and specific laws, with their attention to necessity and proportionality that the European Court requires. Therefore, any police intervention not in accordance with those laws will be regarded as illegal and the evidence as illegally obtained. Illegally obtained evidence, however, need not mean that it will be excluded, as there is no automatic blanket exclusionary rule in the Netherlands. The Dutch Code of Criminal Procedure contained no provisions governing the admissibility of illegally or improperly obtained evidence until 1995, after two rulings (in 1962 and 1978) on these issues by the Supreme Court had established an exclusionary rule. The code emphasises the need to repair irregularities, but where these are irreparable the trial judge has considerable discretion, as clarified by the Supreme Court in 2004 in terms of four options: (i) to note the irregularity but to determine that this had consequences for the fairness of the trial; (ii) to reduce the sentence as form of compensation to the guilty party; (c) to exclude the illegally or improperly obtained evidence; and (iv), if the irregularity means that due process has been fatally compromise, to declare the prosecution inadmissible.[103] Following from its earlier rulings, in 2013 the Dutch Supreme Court clarified the meaning of Article 359a CCP, which deals with the exclusion of evidence: exclusion should only be the sanction if the illegal collection of evidence forms a significant infringement of an important procedural rule and one of the following applies:

1. The illegal collection of evidence means an infringement of the right to a fair trial.
2. If there has been a significant infringement of another important procedural rule or principle and exclusion of the evidence is necessary to prevent comparable infringements.

---

[94] Ibid. at [18].
[95] *Kuruma v The Queen* [1955] A.C. 197.
[96] *R v Sang* [1980] A.C. 402
[97] Ibid at 437.
[98] Police and Criminal Evidence Act 1984, s.82(3).
[99] Ibid, s.78(1).
[100] *R v Walsh* (1990) 91 Cr. App. R. 161.
[101] Ibid. at 164.
[102] Dealing with the detention, treatment and questioning of persons by Police Officers.
[103] HR 30 March 2004, ECLI:NL:HR:2004:AM2533

3. Exceptional situations that demonstrate that such infringements are structural, while the authorities responsible do not appear to have taken sufficient steps to prevent infringement of the rule concerned.[104]

Arguably English and Welsh law has reached a reasonably similar position but by a more circuitous and slower route. With cybercrime policing, case law on the use of an *agent provocateur* (sometimes referred to as "entrapment") could result in potential challenges under PACE. This type of covert activity may be more prevalent in the digital environment where, for example, police agencies take over marketplaces on the dark web[105], create fabricated online profiles or even rely on evidence provided by unregulated third parties[106]. In *R v Sang*, a case which predated the introduction of the PACE exclusionary discretion, Lord Diplock indicated:

> The conduct of the police where it has involved the use of an agent provocateur may well be a matter to be taken into consideration in mitigation of sentence; but under the English system of criminal justice, it does not give rise to any discretion on the part of the judge himself to acquit the accused or to direct the jury to do so, notwithstanding that he is guilty of the offence.[107]

The Runciman Commission (1993)[108] was divided on the admissibility of evidence obtained through what it termed 'pre-trial malpractice or procedural irregularity', with the majority concluding that changing the law of evidence would not necessary improve police conduct:

> In the view of the majority, even if they believed that quashing the convictions of criminals was an appropriate way of punishing police malpractice, it would be naïve to suppose that this would have any practical effect on police behaviour. In any case it cannot in their view be morally right that a person who has been convicted on abundant other evidence and may be a danger to the public should walk free because of what may be a criminal offence by someone else. Such an offence should be separately prosecuted within the system. It is also essential, if confidence in the criminal justice system is to be maintained, that police officers involved in malpractice should be disciplined…..[109]

The majority view, however, may have reflected an assumption of a more interventionist use of the PACE exclusionary discretion than may be the case,[110]as well as perhaps overconfidence in post-facto police disciplinary investigation system (reformed in 2020).[111]

Where the police exercise the investigatory or interception powers available to them they are obliged to record and, where necessary, disclose any information or evidence generated as a result of that investigation. Ultimately the consequences of failing to obtain the correct authorisation or to comply with disclosure requirements would be the potential

---

[104] HR 19 February 2013, ECLI:NL:HR:2013:BY5321.

[105] See for example of the takedown on 20th July 2017 of the dark web marketplaces AlphaBay and Hansa through a coordinated law enforcement operation; https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation <accessed 06/03/2020>

[106] See e.g. CPS legal guidance, Vigilantes on the internet - cases involving child sexual abuse, 03/08/2017, revised 18/03/2018, https://www.cps.gov.uk/legal-guidance/vigilantes-internet-cases-involving-child-sexual-abuse <accessed 06/03/2020>

[107] *R v Sang,* above n.96 at 433.

[108] The Royal Commission on Criminal Justice, *Report* (Cm 2263, 1993).

[109] Ibid. at paras 48-49.

[110] ibid. at para 50.

[111] The leading case, *R v Maxwell* [2010] UKSC 48, revealed 'the gravest police misconduct both before and at trial, and it was persisted in during the first set of appellate proceedings' that had apparently not resulted in either prosecution or disciplinary sanctions. [48]; see also [77-84] and [112-114].

exclusion of the evidence gathered[112] and, in the most serious cases, the discontinuation of the proceedings as an abuse of process.[113] The current legal position in *Maxwell* is that:

> The interests of justice is not a hard-edged concept. A decision as to what the interests of justice requires calls for an exercise of judgment in which a number of relevant factors have to be taken into account and weighed in the balance. In difficult borderline cases, there may be scope for legitimate differences of opinion.[114]

This emphasis on judicial discretion tailored to the circumstances of the case as a "balancing exercise" is very similar to the position reached in Dutch case law, although with regards to cyber-policing and entrapment, the Dutch have partly reached for a different solution. A specific form of "internet-entrapment", the use of a police agent posing as a minor on an internet chat site in order to identify sexual predators, is now specifically authorised by the Computer Crime Act III through a change to the substantive provision that forbids "grooming" (Art. 248e Criminal Code).[115] Making use of what is now known as a "decoy teenager" seems to fall under the special power of the systematic collection of information, requiring authorisation by the prosecutor.[116] The English "balancing act" does little, however, to assist police seeking anticipative guidance in the course of an investigation. In practice, with the policing of cybercrime the problems that this might create may be reduced by the creation of a new regime for regulating communication surveillance and equipment inference, to which we now turn.

d) Centralised quasi-judicial supervision and judicially led inspection of communication surveillance and equipment inference

Convention obligations have resulted in the juridification of police surveillance and interception activities in England and Wales. The Regulation of Investigatory Powers Act (RIPA) 2000 (as amended by the Investigatory Powers Act (IPA) 2016) certainly introduced a more continental style regulation of intrusive law enforcement activity. This process, however, was slow, fragmentary and grudging. It was driven partly by the need to respond to 'serial reverses' at the ECtHR[117] and subsequently in litigation – where a prominent centre-

[112] In the exercise of the Court's exclusionary discretion, PACE 1984, s.78.
[113] Proceedings may be stayed as an abuse of process where it would not be possible for the accused person to receive a fair trial or, where a fair trial is possible, continuing the proceedings would "unacceptably compromise the moral integrity of the criminal justice system", *R v Maxwell,* above n. 113 at [108]. More generally see: A.A. Gillespie '"Paedophile hunters": how should the law respond?' (2019) 12 *Crim. L.R.*, 1016.
[114] *R v Maxwell*, above n. 113 at [19].
[115] This article originally required that grooming activities be directed towards a person younger than 16 years of age, an objective criterion that obviously did not apply to an investigator posing as such a person. After the Court of The Hague had rejected such a case, the Prosecution Service reluctantly ordered that the method no longer be used, but advised the government that the law should be changed to make it possible. The new provision now criminalises grooming in relation to a person younger than 16 or a person posing as such.
[116] On the possible legal problems in the use of this power, see: J.J. Oerlemans 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad*, (2017) 350-359.
[117] P. Roberts, 'Law and criminal investigation' in T. Newburn, T. Williamson and A. Wright, *Handbook of Criminal Investigation* (Willan: Uffcolm, 2007) 101.

left politician and right-wing libertarian made common cause – [118]determined by CJEU;[119] it took some thirty years to put in place.[120] The passage of the second act in particular was not without controversy. Colloquially described as a 'Snoopers' Charter',[121] it was immediately subject to successful challenge in the High Court.[122] (The Dutch Computer Act III also led to criticism because of its potential impact on privacy rights, while the Dutch Federation of Journalists vented worries about the possible use of hacking powers with regard to on-line journalists and the consequent circumvention of guarantees of the freedom of expression.)[123] The criticisms levelled at IPA primarily related to the powers of bulk interception of communications data and the analysis of that data through the use of targeted examination warrants. Cumulatively, these criticisms and successful legal challenges eventually led the government to abandon intermediate legislation,[124] redraft elements of the legislation and, following consultation, to issues redrafted Codes of Practice[125].

The result of this considerable amount of litigation, legislation and political argument is juridification in a very English guise. The Act of 2016 resulted in the consolidation of supervisory and regulatory expertise, with the merger of the Office of Surveillance Commissioners, the Intelligence Services Commissioner and the Interception of Communications Commissioner into the Office of the Investigatory Powers Commissioner (IPCO).[126] In addition the Office for Communications Data Authorisations (OCDA) was created so that the authorisation of targeted communications data could be transferred from Home Office officials to 'an independent arm's length body'. This is still financed and staffed by the Home Office, but its CEO is responsible to the Investigatory Powers Commissioner, always a senior member of the judiciary, and not Home Office ministers and senior officials. In short the post-IPA regime consists of highly centralised judicial supervision over current police investigations, retrospective compliance inspections of police forces, and anticipative guidance both in formal published codes and more informal contributions to police training and national conferences.

This unified organisational structure was matched with a similar consolidation of the Investigatory Powers Commissioner's remit and IPCO staff, consisting of judicial commissioners (15 at the time of writing) and inspectors. A single group of national specialists now oversee – through warrant authorisation and inspections – communications data interception, surveillance and equipment interference ('hacking') by the police, and also, depending on the regulated powers, agencies with police (NCA) or regulatory functions (HRC), the intelligence agencies and municipal government. Within this comprehensive framework the levels of seniority and the proportionality test for authorising surveillance etc.

---

[118]The UK litigation that culminated in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* [2016] ECLI:EU:C:2016:970 was initiated in the name of the then leader Deputy leader of the Labour Party and MP , Tom Watson and David Davis MP, a libertarian Conservative who ceased to be a party to the litigation when he joined the UK Government as the holder of the office of Secretary of State for Exiting the EU.

[119] *Watson* and an earlier a successful challenge before the High Court (*David Davis and others -v- Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) resulted in the repeal of the Data Retention and Investigatory Powers Act 2014 (DRIPA).

[120] The litigation began at Strasbourg with *Malone v UK* [1985] 7 EHHR 14 and culminated at Luxembourg in 2016with *Watson*

[121] https://www.libertyhumanrights.org.uk/human-rights/privacy/snoopers-charter < last accessed 06/03/2020>

[122] *The Queen on the application of the National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department, Secretary of State for Foreign and Commonwealth Affairs* [2018] EWHC 975 (Admin)

[123] /www.villamedia.nl/artikel/kritiek-op-wet-computercriminaliteit-iii < last accessed 7 May 2020

[124] The Data Retention and Investigatory Powers Act 2014 (DRIPA), which was replaced by IPSA.

[125] IPA 2016, Schedule 7, Codes of Practice < https://www.gov.uk/government/consultations/investigatory-powers-act-2016 > last accessed 06/03/2020.

[126] *Annual Report of the Investigatory Powers Commissioner 2017*, (IPCO: London, 2019).

and also the inspection regimes vary to reflect different levels of intrusiveness and sensitivity. For the police forces, these two statutes introduced a common legal and organisational framework for the regulation of both digital and covert human intelligence sources (informers),[127] thus ensuring similar approaches to proportionality, necessity and record keeping in both online investigations and 'real world' surveillance and intelligence operations.

There is a considerable awareness within IPCO that in many countries with broadly equivalent oversight bodies the authorisation and inspection functions are divided between separate organisations. The combination of oversight and review functions is seen, however, as a major strength. 'The 15 judicial commissioners are able to identify areas which merit particular scrutiny on inspection, and the inspectors are well placed to inform the judicial commissioners of the issues of relevance to future applications for warrants that were identified on inspections.'[128] IPCO intend to inspect all UK LEAs annually and, as new system came into operation, 39 authorities were inspected in 2018,[129]

Summary of argument and conclusions

We started this article in the expectation that a comparison of cyber-policing in England and Wales and the Netherlands should reveal some interesting differences and possible similarities that would afford greater insight into the problems the advent of cybercrime pose for the police wherever they may be. There appear to be similarities in abundance, in particular in the growing attention paid to cybercrime, in the attempts to legislate specifically for cyber-policing and in the notion that rules and regulations designed to combat (organised) crime in the real world can be adapted to fit the policing of cyberspace. At first sight, those rules also appear similar, as with regard to surveillance, the non-recognition of traditional jurisdictional boundaries and the need to obtain authorisation. It is also interesting to note that neither country really pays specific attention to the potentially extra complications of policing the dark web. Although the Netherlands has a dark web police team, the Explanatory Memorandum to the Computer Crime Act III merely mentions Tor as a potential complicating factor. It may well be that the very name "*dark* web" conjures up such connotations of dangerous, invisible crime, impossible to police, that the legislatures of both countries are unwilling to burn their fingers trying to come up with solutions. At the same time, the powers to ignore the usual territorial jurisdictional restraints granted to both the Dutch and the English police (and in the USA and other European countries), are particularly suited to crime-fighting on the dark web and getting round the encryption barriers of the TOR network.

Although the similarities are many, there are still several important and often subtle differences between the Netherlands and England and Wales that reflect the underlying ideology of policing, its influence on police (organisation) and legal culture, and the difference between inquisitorial and adversarial procedure. Whereas the Dutch police are thoroughly aware of the importance of a basis in law for any activity that might infringe on individual rights and freedoms, especially privacy (in particular since this point was publicly rubbed in during the 1990's scandal, see above), it is not uncommon to hear senior English police officers emphasising that the police in England and Wales are police of and for the people – and that they may therefore do anything that is not expressly forbidden.[130] It is

[127] RIPA Part II.
[128] Investigatory Powers Commissioner, *2017Annual Report* (IPCO: London, 2019) para 2.11
[129] Investigatory Powers Commissioner, *2018 Annual Report* (IPCO: London, 2020) para 11.5.
[130]. Reflects comments and discussion noted during empirical research, including Chatham House Rule NPCC organised conferences on 22-25 October 2018 and 19-21 November 2019.

perhaps psychologically easier to remember that nothing is allowed unless it is permitted by specific legislation, than to know that everything is allowed, but may be forbidden somewhere. The Dutch police are helped by the fact that in the Netherlands, the rules of covert policing are to be found where all other rules on the use of explicit police powers reside, in the Code of Criminal Procedure and in a prosecution directive that clarifies ambiguities, with specific powers outlined in the Computer Crime Act III. As is often the case in in England and Wales, such rules have grown by accumulation and have been laid down in several different pieces of legislation and case law.

Despite the existence of guidance and the growing importance of Article 8 ECHR in the context of criminal procedure in England and Wales following S and Marper v the United Kingdom[131] and the approach of, in particular, the UK Supreme Court to the question of necessity/proportionality in respect of the interference with Article 8, UK police culture does not seem to be fully imbued with the automatic reflex of Continental police forces to ask where the power they wish to employ is regulated and whether its use would be proportionate. Where the Dutch police need guidance is in knowing just how real world powers relate to policing the Internet and how to technically employ them. This may also apply to the police in England and Wales, but here there is also uncertainty as to where to find such powers and what they mean, which creates a strong imperative for clear policies and procedures to demonstrate the necessity/proportionality of any interference. Where these seem to have been given some body in the post-IPA regulatory regime, that too is fragmented, at least compared to the Dutch situation where centralised criminal justice authorities provide both authorisation when required and continuous oversight in each case rather than periodic inspection. Partly this is due to the Dutch concept of criminal justice being broader than that in England and Wales. In the Netherlands, criminal justice relates to the processing of criminal offences. It is linked to behaviour (the offence) and not to the agency that deals with it. The powers of covert (internet) policing may be employed by many agencies (e.g. tax and financial authorities, border control agency, environmental agencies). They are triggered by the (seriousness) of a criminal offence and all are governed by the same rules and subject to authorisation and oversight by the prosecutor and, should prosecution ensue, by the courts. Where the English and Welsh system post IPA is now centralised, the Dutch equivalent is both centralised and unified, with a, traditionally, highly powerful Public Prosecution Service at its core (this does not apply to the Security Services that are subject to a different regime, although security service information does sometimes end up in court as evidence).

As is to be expected, further differences between the countries are to be found in the nature of the safeguards that ensure the legality and legitimacy of cyber/policing. It will be clear that in accordance with the principles of policing and inquisitorial procedure, great store is set in the Netherlands by scrutiny and monitoring of police activity (predominately by the prosecutor) to make sure that it does not unnecessarily infringe on individual rights, that it conforms with the law and, should it come to a prosecution, that any evidence thus collected will be logged in full, is reliable and can be used in court. Such safeguards, with a high investment in the presumed impartiality of the inquisitorial prosecutor, exist in particular during the pre-trial investigative stage of criminal process, meaning that oversight does not rely on the case coming to trial as it does in England and Wales, and that the prosecutor will be in a position to know the ins and outs of an ongoing police investigation, or an investigation by any other investigative agency. This of course presumes that the prosecutor is (technically) knowledgeable enough to be able to judge the necessity and proportionality of the measures and methods the investigators wish to employ and that the court will also

[131] *S and Marper v United Kingdom* [2008], ECHR 1581; Application nos. 3056.

understand them. English adversarial process relies on irregularities being brought to light by the defence in adversarial debate during trial, which explains the supreme importance of disclosure. If there is no trial, there will be no scrutiny of the police investigation by anyone external to the police organisation. But, again, this depends on knowledge and understanding on the part of defence counsel and on full and complete disclosure.

It should however be noted that in both countries there is an issue with knowledge of and insight into cyber/policing and not only with regard to prosecutors, defence lawyers and the judiciary who must be able to judge the legality of the evidence. Where both countries depend on warrants to ensure the legality of investigative measures, this presupposes that the issuing authority will also be able to do the same. This has proved to be a problem in the Netherlands concerning "ordinary" covert policing, in particular in relation to telephone taps, which require authorisation by the judge of instruction. When the Special Investigative Powers Act was evaluated after five years, it became apparent that each tier of scrutiny relied upon the previous one to have done its job properly, so that judges of instruction relied on the prosecutor and the trial courts on the judge of instruction and, more generally, on the internal methods of scrutiny built into the Act. The issuing of warrants was found to have become something of a rubber-stamping exercise, with trial judges unable or unwilling to question decisions made by previous authorities.[132] This is perhaps a particular problem of inquisitorial procedure, which, functioning as it does in an environment almost devoid of external controls and with far fewer defence rights than is usual in adversarial procedure, in essence "polices itself"[133]

There is one area in which the Dutch police seem to be at an advantage, and that is in the organisation of the police. Greater centralisation seems to provide more coherent policies and priorities and to promote specialised knowledge at all levels, something the UK police consistently emphasise as lacking, while they also complain that specialised branches have a monopoly on knowledge. There is no expectation of organisational centralisation and common policies among the heads of the disparate UK forces.[134] It would indeed be going against the historical and cultural grain to expect the sort of centralisation and division of labour foreseen by Stol and Strikwerda (see notes 42 and 47 *supra*). Which brings us to our final point.

It is sometimes assumed that legal comparison helps identify best practices that can then be transferred from one country to another. This is usually a question of wishful thinking, or ignorance of the underlying systemic legal-cultural factors that make legal transplants a hazardous undertaking. What comparisons can do is help identify bottlenecks and barriers to improvement by examining the underlying issues that make the law and its enforcement what it is in any given country. In that way, it may point to what is and is not possible, at least in the short term. And so it may well prove with cyber-policing. If this contribution has managed to make a start, we are well-pleased.

---

[132] A. Beijer *et al. De Wet bijzondere opsporingsbevoegdheden – eindevaluatie*, Boom Juridische uitgevers/Ministry of Justice (Meppel: The Hague, 2004) 159-192.

133 See on this point C. Brants and S. Field, 'Truth-finding, procedural traditions and cultural trust in the Netherlands and England and Wales: when strengths become weaknesses' (2016) 20 *International Journal of Evidence and* Proof 266-288.

[134] Noted repeatedly during our research, including at Chatham House Rule NPCC organised conferences on 22-25 October 2018 and 19-21 November 2019. The reluctant recognition that the police force structure is unlikely to change stems from a failed attempt in 2006 to amalgamate the 43 territorial police forces into 24 larger units. This had significant professional support, but the cost of implementation was judged too expensive and it met with strong popular opposition, see, for example: I. Blair, *Policing Controversy* (Profile Books: London, 2009) 295-6. It is also significant that governments over two decades have concentrated on policies that have a '"calculative and contractual mode" of shaping [police] "independence" albeit at a local rather than national level', B. Bowling, R. Reiner and J. Sheptycki (quoting L.Turner), above n.29 at 249.

Funding

The author(s) received financial support for the research, authorship, and publication of this article from NordForsk, the Economic and Social Sciences Research Council (ESRC) and the Netherlands Organisation for Scientific Research (NWO) as funding for Police Detectives on the TOR-network: A Study on Tensions Between Privacy and Crime-Fighting (project no. 80512).