scripted

Volume 9, Issue 3, December 2012

CRIMINAL LAW AND CYBERSPACE AS A CHALLENGE FOR LEGAL RESEARCH

Bert-Jaap Koops[*]

Abstract

The Internet transforms crime and crime-fighting, which has fundamental implications for the law and legal research. Since online and offline activities are seamlessly integrated, cybercrime is no longer a specialist field but affects the core of 21st-century criminal law. The transformation of crime exposes gaps in substantive and procedural criminal law, creating three types of challenges. First, regulatory challenges, e.g., how to deal with sovereignty and jurisdiction conflicts in borderless cyberspace. Second, normative challenges, such as value conflicts related to Internet content. Third, technological challenges, related to secure computing and value-sensitive design. The interplay of these challenges should lie at the heart of criminal-law research in the cyberspace age.

Classic legal research often addresses problems in a one-dimensional manner: the law is taken as a given and then applied to a societal issue, or a social development is used to argue why and how the law should change. However valuable such research can be, legal research needs to factor in the role that technology increasingly plays in law and society, as well as the process of the mutual shaping of regulation, technology, and society. This calls for multidisciplinary research aiming for prudent solutions to regulatory problems. If criminal law is to stay abreast of the 21st century challenges of crime permeated by cyberspace, dogmatic understanding of the criminal law system itself no longer suffices. Rather, researchers need to be well-versed in regulation theory, adopting concepts like the regulatory tool-box and multi-level governance, to meet the challenges of globally, digitally networked crime.

DOI: 10.2966/scrip.090312.354

[*] Professor of Regulation and Technology, TILT – Tilburg Institute of Law, Technology, and Society, Tilburg University, The Netherlands.

1. Introduction

The media regularly report stories of different forms of cybercrime, with varying degrees of seriousness. The lonesome hacker who manages to penetrate the system of a multinational and who copies a customer-record database. The group that calls itself Anonymous, blocking websites of companies that do things Anonymous don't approve of (such as cutting off payments to WikiLeaks). The mysterious virus that brings down Iranian power-plants. The clumsily phrased email, asking to 'contact attorney Mzulukwulu to retrieve your inheritance' from a Zambian widow you've never heard of.

However fascinating such examples are, should they be of interest to anyone but the odd specialist in law & technology studies? Do not the average criminal lawyer and the average legal researcher have to address rather more important things, things that happen in the real world and that have physical rather than virtual consequences?

I would argue that the answer to both questions is no. Cyberspace should interest everyone who is involved in criminal law. The classic view of cybercrime, centred on the lonesome, nerdy hacker, is largely based on fiction, a fiction from the 1980s and 1990s.[1] Reality has changed dramatically, causing a step-change in cybercrime and its consequences for the 'real world'.[2] Cybercrime is no longer about peer reputation among whiz kids, it's all about money – big money. A considerable black market caters for all kinds of criminals, where you can buy a bunch of credit-card numbers (including the codes on the back) for a couple of dollars, or rent a network of zombie computers for an hour to spread your spam or block your favourite villain's website.[3] Moreover, as the Internet integrates seamlessly into our economy, politics, and social life, any attack on or from cyberspace is an attack on the real world. Cybercrime is real crime, and increasingly, real crime has a cyber-element to it.

In this paper, I want to investigate the challenges that cybercrime and cyberspace bring to the law, and consequently also to legal research, based on the premise that the Internet has become so fundamental a part of life that it can no longer be ignored by criminal law or research in criminal law. After sketching the characteristics of the Internet and cybercrime and highlighting some tensions that these bring to the functioning of criminal law (section 2), I will discuss the consequent challenges for law and legal research. At a conceptual level, these challenges are threefold in character: regulatory, normative, and technical. The challenges are inextricably intertwined, however, and I argue that it is the mutual shaping of regulation, norms, and society that should be the focal point of analysis (section 3). This leads to the conclusion that criminal-law research requires a broad perspective on regulation and a multidisciplinary approach (section 4).

---

[1] D Wall, "Cybercrime and the Culture of Fear: Social Science Fiction and the Production of Knowledge about Cybercrime" (2008) 11 *Information, Communication & Society* 861-884.

[2] D Wall, *Cybercrime. The Transformation of Crime in the Information Age*, (Cambridge: Polity, 2007).

[3] B Sandywell, "On the globalisation of crime: the Internet and new criminality" in Y Jewkes and M Yar (eds) *Handbook of Internet Crime,* (Cullompton: Willan Publishing, 2010) 38-66, at 51.

2. The Internet, Cybercrime, and Criminal Law

2.1. The Opportunity Structure for Cybercrime

The Internet is global and allows for real-time connections between people regardless of their location. Hence, time, distance, and borders are much less important than in traditional crime. Being a network of networks that allows for automated processing and transfer of digitised data at the speed of light, on an unprecedented scale, the Internet is transforming many aspects of society. Because of these characteristics, it also provides special opportunities to commit crimes, which is important from a criminological perspective:

> Routine activity theory (and, indeed, other ecologically oriented theories of crime causation) thus appears of limited utility in an environment that defies many of our taken-for-granted assumptions about how the socio-interactional setting of routine activities is configured.[4]

Crime in which computer networks are the target or a substantial tool are usually called 'cybercrimes'. The committing of these crimes is facilitated by a combination of many characteristics of the Internet, which together create a unique opportunity structure for cybercrime. These characteristics are: global reach, deterritorialisation, flexible network structure, anonymity, distant offender-victim interaction, manipulability of data, automation of crime, massive scale, aggregation of negligible damages, targeting information as a commodity, limitations to capable guardianship, and rapid innovation cycles.[5]

This opportunity structure supports the suggestion that 'cybercrime' does indeed represent the emergence of a new and distinctive form of crime.[6] Even if cybercrime to some extent recreates traditional forms of crime, such as fraud, theft, and sabotage – representing old wine in new bottles – its scale and variety imply that 'we are dealing with *an awful lot of wine* in very many, differently shaped and capacious bottles'.[7]

Convictions for these crimes are still relatively rare (compared to other crimes), but this does not mean cybercrime is not prevalent.[8] Theory and anecdotal evidence suggest that cybercrime is becoming organised, large-scale, diversified with increasing division of labour, and it is expected to develop increasing ties with offline

---

[4] M Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory" (2005) 2 *European Journal of Criminology* 407-427, at 425.

[5] BJ Koops, "The Internet and its Opportunities for Cybercrime" in M Herzog-Evans (ed) *Transnational Criminology Manual, Vol. 1,* (Nijmegen: WLP, 2010) 735-754, at 740-741.

[6] M Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory" (2005) 2 *European Journal of Criminology* 407-427, at 407.

[7] Y Jewkes and M Yar, "Introduction: the Internet, cybercrime, and the challenges of the 21st century" in Y Jewkes and M Yar (eds) *Handbook of Internet Crime,* (Cullompton: Willan Publishing, 2010) 1-8, at 3.

[8] RG Smith et al, *Cyber criminals on trial*, (Cambridge; New York: Cambridge University Press, 2004), at 25-29.

organised crime.[9] Indeed, because of the network effects of globalisation, the information economy, and the automation of victim-offender relationships, the Internet is transforming the way crime is being committed, resulting in a move from traditional, physical crime in the direction of cybercrime.[10]

2.2. Cybercrime and Criminal Law

Sometimes, cybercrimes can be relatively easily dealt with in the existing legal system. A cyber-variant of a traditional crime can be punishable under an existing provision, such as forgery,[11] or it can be made punishable by reformulating the provision (e.g., by adapting the provision on fraud to include obtaining computer data through false pretences). However, it is not easy to bring more computer-specific offences, such as those targeted at the confidentiality, integrity, or availability of computer systems, under traditional provisions, so that computer-specific offences need to be introduced in the criminal law. And legislatures cannot rest at that: on-going developments in computer technology require the legislature to remain ever vigilant to fill gaps in criminalisation, for example, to deal with new forms of identity theft or search-engine manipulation.

More important even than gaps in substantive law, are potential limitations in procedural law. The existence of 'data havens'- countries in which certain forms of cybercrime are not penalised, and which therefore cannot provide mutual legal assistance in the absence of double criminality - is a familiar spectre in cybercrime debates. Moreover, mutual legal assistance is traditionally too slow to deal with investigation in cyberspace, where evidence can be destroyed with a few mouse clicks or moved from Belgium to Belize within seconds.

National and international legal instruments are doing their best to fill existing gaps in substantive and procedural law. For example, the Council of Europe's Cybercrime Convention[12] has done a good job in ensuring minimum levels of adequate legislation and enhancing mutual assistance among the currently thirty-seven party states, and it is serving as a model for legislation in non-member states as well.

But the problems go deeper than possible gaps in substantive and procedural law. First, cybercrime challenges some fundamental concepts of criminal law. In the 1980s and 1990s, many countries discussed whether computer data should be considered property, mainly with a negative answer, since data are intangible and multiple while property is more physical and has unique ownership. The issue seemed to have been addressed satisfactorily, but is now back on the agenda with the advent of 'virtual goods', such as objects with unique ownership in online games or virtual worlds that are worth real-world money. The Dutch Supreme Court recently ruled that, depending

---

[9] BJ Koops, "The Internet and its Opportunities for Cybercrime" in M Herzog-Evans (ed) *Transnational Criminology Manual, Vol. 1,* (Nijmegen: WLP, 2010) 735-754 at 744-745.

[10] D Wall, *Cybercrime. The Transformation of Crime in the Information Age*, (Cambridge: Polity, 2007).

[11] For a leading Dutch case, see Hoge Raad [Supreme Court] 15 January 1991, *Nederlandse Jurisprudentie* 1991, 668.

[12] Convention on Cybercrime, Budapest, 23 November 2001, CETS 185.

on the circumstances, such virtual goods could be the object of theft,[13] thus considerably expanding, or at least re-interpreting, the notion of 'property' in criminal law. Another example of challenged concepts, at a different level, is the *de minimis* principle that behaviour should only be criminalised if it causes more than a minimum level of harm. Some forms of cybercrime may not pass this minimum threshold for individual persons. For example, a computer virus that slows down your computer and that requires some effort to remove, but because millions of people can be affected, the net result could constitute considerable harm at a societal level. And even if the act is punishable in theory, which country will take up investigation and prosecution if a relatively small portion of the global victims, each with small amounts of harm, lives in its jurisdiction?[14]

Second, the investigation of cybercrimes poses considerable problems. Even disregarding the issue of cross-border investigation and mutual legal assistance, investigating and prosecuting a cybercriminal requires substantial effort as well expertise, both of which, in a context of scarce resources, could be dedicated to other crimes that are easier and more efficient to prosecute, or that rank higher on the political agenda. Finding and securing digital traces is a specialist job, and even if sufficient digital evidence of a cybercrime is found, this usually traces back to the perpetrator's computer, but not necessarily to the person who was behind the computer at the material time. There is also a lack of formal standardisation or legal procedures for collecting, preserving, and presenting digital evidence, thus calling the evidence's reliability into question.

Third, and perhaps most importantly, cyberspace confuses the boundaries of criminal law. Increasing attention is being paid to cyber-warfare, in addition to risks of cyber-terrorism which have been recognised for some time. The doctrinal distinction between crime, terrorism, and international armed conflicts hinges on the perpetrator (an individual, a group, or an organisation associated with a state?) – and his motivation (personal gain, implanting terror, disrupting society or overthrowing the government?). While this distinction theoretically also applies to the cyber-variants of crime, terrorism, and warfare, it is very difficult to ascertain who exactly is behind a cyber-attack and what exactly the attacker's motivation might be. The difficulty of attribution presents immense challenges in fashioning an appropriate legal response. For example, which institution should take the lead in the response – the public prosecutor, the security agency, or the ministry of defence?[15] But also closer to the area of criminal law itself, the Internet facilitates state interventions that cannot be neatly categorised as a criminal investigation, a prosecution, or an execution of sanctions. Intelligence-led policing, with large-scale data collection and data mining in its wake, is often not targeted at a specific crime but rather at wide-ranging groups of 'interesting people'. Resulting interventions are not necessarily focused on preparing a criminal trial, but at taking certain administrative decisions or at simply disrupting possible criminal behaviour. Such practices of criminal law do not fit well in the traditional scheme of crime → investigation → criminal trial → criminal

---

[13] Dutch Supreme Court [Hoge Raad] 31 January 2012, LJN BQ9251.

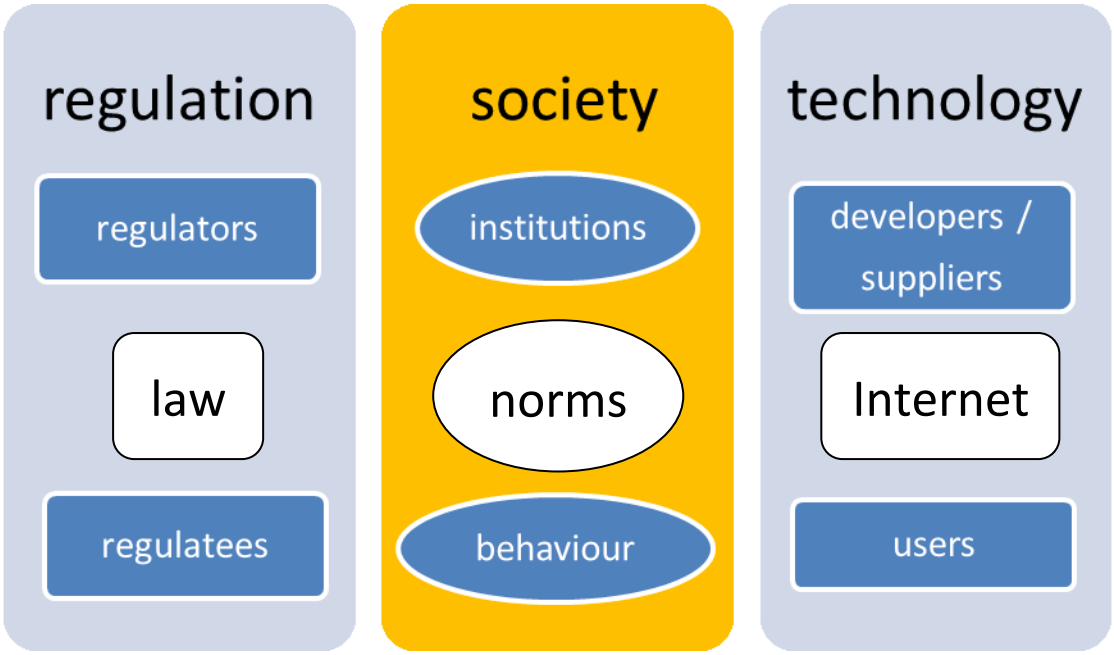
[14] See generally on the *de minimis* problem, D Wall, *Cybercrime. The Transformation of Crime in the Information Age*, (Cambridge: Polity, 2007).

[15] SW Brenner, *Cyberthreats: the emerging fault lines of the nation state*, (Oxford; New York: Oxford University Press, 2009).

sentence. This requires us, among other things, to rethink the legal protection of citizens in the form of new checks and balances in the criminal legal system.[16]

3. Challenges for Law and Legal Research

While the previous section highlighted some of the more fundamental problems that criminal law faces through the Internet and cybercrime, here I want to tie these problems together at a conceptual level, in order to better understand the challenge of cyberspace for law and legal research. The aim of law is to regulate society, and criminal law is a particular type of law meant to address particularly pressing social problems that other regulatory instruments cannot sufficiently address themselves. While (criminal) law mediates between regulator and regulatees, technology mediates between developers or suppliers of technology and technology users. Moreover, the behaviour of people – regulatees and technology users – is also shaped by the norms embedded in particular social contexts, often in the form of institutions (cultures, traditions, practices). This can be schematised as follows:



I suggest that the challenge of cyberspace to the law and legal research is found in all three dimensions of this scheme. Thus, we can distinguish regulatory, normative, and technical challenges. I will illustrate each dimension of the challenge by discussing some illustrative examples in the following sections.

3.1. Regulatory Challenges

One of the most fundamental tenets in criminal law is national sovereignty. More than any other area of the law, criminal law is tied up both with the cultural values of a nation and with the sovereign exercise of power over citizens on a territory. There is

[16] BJ Koops, "Technology and the Crime Society: Rethinking Legal Protection" (2009) 1 *Law, Innovation & Technology* 93-124.

an obvious tension between the global character of the Internet and the nation-based exercise of criminal law. The practical solution regulators have found to deal with this tension is to harmonise national laws and to co-operate with mutual assistance as much as possible.[17] But 'as much as possible' leaves much room for national divergence. Is this pragmatic approach, which does little to address the issue of national sovereignty, sustainable in the longer term?

Around the year 2000, two Russian citizens, Alexey Ivanov and Vasily Gorshkov, were lured to the United States by the FBI, who tricked them into giving their passwords and subsequently accessed their Russian computers to obtain evidence of hacking. The US court convicting Gorshkov and Ivanov found that Russian law had not been violated by the extraterritorial FBI search; however, Russia filed charges against the FBI officials for hacking computers on Russian territory.[18] A similar discrepancy of views on sovereignty can be seen in countries collecting data stored abroad by asking the voluntary help from service providers, such as Google, to retrieve someone's e-mail messages. According to Art. 32(b) of the Cybercrime Convention, this data collection is lawful if the service provider is in the lawful position – typically stipulated in the general terms and conditions – to forward the data to the foreign authorities. This is contested, however, not only by Russia but also by Slovakia and Ukraine, both parties to the Cybercrime Convention.[19] This illustrates fundamental differences of opinion among regulators about how Internet searches should be regulated, based on diverging interpretations of threats to national sovereignty.

Another example of cybercrime's challenge to sovereignty can be seen in jurisdiction claims over cybercriminal acts. While most countries claim jurisdiction based on the location of the act, including its effects, and sometimes on grounds of nationality of the perpetrator or victim, some countries have extremely wide-reaching jurisdiction claims.[20] Malaysia's Computer Crime Act applies "if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time".[21] Since all computers nowadays – including smartphones – are 'capable of being connected' to a Malaysian computer, any cybercrime can in theory be prosecuted by the Malaysian authorities. Even without such broad provisions, jurisdiction might easily be established over foreign websites. In the case of Joseph Weiler, a US journal editor who was sued in France for an allegedly defamatory book review, the French court applied the standard that the book review, hosted in the US, should be considered to

---

[17] U Sieber, *General Report on Internet Crimes for the 18th International Congress of the International Academy of Comparative Law Washington D.C. 2010,* (2010) at 83-85.

[18] See JR Herrera-Flanigan, "Cybercrime and Jurisdiction in the United States" in BJ Koops and SW Brenner (eds) *Cybercrime and Jurisdiction,* (The Hague: TMC Asser Press, 2006) 313-325, at 322-323.

[19] The Cybercrime Convention Committee (2008) *Compilation of responses to questionnaire for the parties concerning the practical implementation of the Cybercrime Convention*. T-CY (2008) 01, Strasbourg, 11 March 2008 at 28; Committee of Experts on the operation of European conventions on co-operation in criminal matters (2008) *Replies on Mutual Legal Assistance in Computer-Related Cases*. PC-OC (2008) 09rev, Strasbourg, 1 December 2008 at 6.

[20] SW Brenner and BJ Koops, "Approaches to Cybercrime Jurisdiction" (2004) 4 *Journal of High-Technology Law* 1-46.

[21] Art. 9 Malaysia Computer Crimes Act.

have been published in France, and therefore falling under French jurisdiction, if the book review "[were] accessible from France or [were] actually consulted in France" at the material time. Since the complainant in this case had not provided evidence that someone from France had actually consulted the website, France did not have jurisdiction.[22] Yet this standard implies that if someone *can* provide evidence that a foreign website was accessible in a certain country – which is easy to do – that country can claim jurisdiction over the website.

Such provisions not only raise questions about the adage that every citizen is supposed to know the law (should Internet users study the laws of all countries which they "are capable of connecting to" when entering cyberspace?) but also about jurisdiction conflicts, arising from the fact that many countries can claim jurisdiction over a cybercrime at the same time.

These examples may serve to illustrate the regulatory challenge that cyberspace poses to national sovereignty as a fundamental element of criminal law. While countries are very hesitant to give away sovereignty by allowing foreign criminal investigations in its territory, but at the same time rather liberal in claiming jurisdiction over cybercrimes, tensions such as those between Russia and the US are bound to emerge more often as cybercrime continues. Legal research has a prime topic here to try and find ways to make global cybercrime-fighting compatible with the political reality of national sovereignty.

3.2. Normative Challenges

Yahoo! hosted a website where Nazi memorabilia were offered for sale. Although the website was hosted on US servers, Yahoo! was taken to a court in France by the Ligue contre le racisme et l'antisémitisme and the Union des étudiants juifs de France. The French court found the website in violation of the French Criminal Code and ordered Yahoo! to make the website inaccessible to French netizens. Yahoo! subsequently went to a US court to claim its First Amendment right to publish the website. The District Court ruled the French verdict to be inapplicable in the US. This was overturned by the Court of Appeals which found that the court had no personal jurisdiction over the French litigants.[23] Although the French court only ordered Yahoo! to make the content unavailable to French users, the service provider chose to take down the site altogether.

The case is an eminent illustration of the conflict of values that may emerge on the Internet, where content that is lawful in one country can be illegal in another. This has led to an increasing use of geolocation to fine-tune Internet content to the country (or states in a federal jurisdiction) of website viewers.[24] Nowadays, most Internet

---

[22] Tribunal de Grand Instance de Paris 3 March 2011, Public Prosecutor v Weiler, unofficial translation available at http://www.ejiltalk.org/wp-content/uploads/2011/03/Public-Prosecutor-v-Weiler-judgement-March-3-2011-3.pdf (accessed 28 Oct 2012).

[23] Tribunal de Grande Instance Paris, 20 November 2000; United States Court of Appeals, Ninth Circuit, 433 F.3d 1199 (*Yahoo! Inc.* v. *LICRA and UEJF*), 12 January 2006.

[24] See, e.g., JR Reidenberg, "States and Internet Enforcement" (2004) *Univ. of Ottawa Tech. L. J.* 213ff; J Mason Kjar, "2 Obscenity Standards 1 Neat Solution How Geotargeting Extends Traditional Obscenity Law to the Internet" (2012), *Case Western Reserve Journal of Law, Technology & the Internet* 2(2).

Protocol (IP) addresses are fixed and traceable to a certain country that distributed the IP address, which enables the service provider to recognise the geographic origin of web-users. As a result, Google, for example, shows different search results for certain terms depending on whether one uses google.de, google.nl, or google.com. Still, it is challenging, perhaps even impossible, to satisfy all countries' normative standards for content. Many Asian countries, for example, have provisions outlawing pornography or other content considered immoral, often using fuzzy terms that can be interpreted according to current moral standards. For example, the Indonesian Information and Electronic Transactions Act prohibits the distribution or causing to be accessible of 'electronic information and/or electronic documents with contents that violate decency [*kesusilaan*]'.[25] Of course, service providers are in no position to determine which content violates current Indonesian standards of decency, and geolocation technologies will therefore not help to prevent conflicts over website content in different value systems.

Another key example of conflicting values is the online battle over intellectual property rights (IPR), where Internet users, activist groups, content providers, and collective IPR organisations have rather different views on what are acceptable forms of content sharing. This has not only led to courts ordering ISPs to block access to file-sharing websites, but also to laws, such as the French HADOPI, requiring access providers to cut off users from the Internet if they systematically infringe copyrights.[26] The value conflict between (intellectual) property and free access to information will continue to rage for a considerable period of uncertainty, which will see varying legal instruments for stricter copyright enforcement as well as new business models for innovative content exploitation.[27]

What these examples illustrate is a key normative challenge in cybercrime law and research. That is, how to reconcile the existence of varying local value systems with the global spread of content that is one of the core assets of the Internet? This question lies at the heart of what Brownsword terms 'regulatory cosmopolitanism', or the aim of globally safeguarding fundamental or universal values with an appropriate margin for legitimate local differences, arguably one of the most fundamental challenges in Internet regulation.[28]

3.3. Technical Challenges

The Internet has evolved since the 1960s into an extremely complex network with a variety of protocols to route traffic as efficiently and robustly as possible. The open character of the Internet, with its focus on 'intelligence at the ends' – add-ons of

---

[25] Art. 27 of Law No 11 of 2008 (translation by Dewi Avilia). A similar provision is found in article 282 of the Indonesian Criminal Code.

[26] See T Rayna and L Barbier, "Fighting Consumer Piracy with Graduated Response: An Evaluation of the French and British Implementations" (2010) 6 *International Journal of Foresight and Innovation Policy* 294-314.

[27] S Katyal, "Filtering, Piracy Surveillance, and Disobedience" (2009) 32 *Columbia Journal of Law and the Arts* 401-426.

[28] R Brownsword, "Regulatory Cosmopolitanism: Clubs, Commons, and Questions of Coherence" (2010), TILT Law & Technology Working Paper No. 018/2010, http://ssrn.com/abstract=1715445 (accessed 28 Oct 2012).

applications and content by end-users – rather than in the infrastructure itself, comes with the downside of making it difficult to prevent malicious exploitation of weaknesses in the system. If we were to build the Internet now, it would be possible to devise an infrastructure that is much more robust against malware and network attacks, but the historical legacy of the Internet does not allow us to rebuild it from scratch. The challenge, therefore, is to build in security without curtailing too much of the openness of the existing system.[29]

Several fields take up this challenge by focusing on technical solutions, such as non-manipulable end-user software and hardware[30] or mandatory authentication of Internet users.[31] Such solutions, however, face substantial obstacles of scalability, industry or user adoption, and the impossible-to-exclude possibilities for circumvention by malicious users. As a result, some proposals rely on a combination of technical measures with user education, even including the ultimate remedy of making end-users criminally liable for insufficient computer security if that leads to their computers being abused by others to commit cybercrimes.[32] Although user education may help to obtain a reasonable level of average security, cybercrime often exploits vulnerabilities in ways too sophisticated to be blocked by your average firewall or virus scanner. Enforcing criminal liability on zombie-computer owners for being an accessory to cybercrimes is therefore unfair and ultimately ineffective as a punitive measure. But how then should the responsibilities be distributed over the various Internet actors to improve computer security? A key technical challenge is to come up with robust and scalable security measures that are compatible with a fair distribution of responsibilities and liability among technology developers, intermediaries, and end-users.

3.4. The Mutual Shaping of Regulation, Society, and Technology

Distinguishing between regulatory, normative, and technical challenges may be a helpful way of putting the challenge of cyberspace to criminal law into perspective. Generally speaking, these challenges address different stakeholders: regulators, society, and technology developers, respectively. However, the distinction is artificial, in that the illustrative challenges I described are not restricted to a single dimension or to a single stakeholder. Indeed, to solve the puzzles one needs to engage with all dimensions to get the whole picture. For example, the issues of sovereignty in cross-border criminal investigation and jurisdiction over cybercrimes (described above as a primarily regulatory challenge) closely relates to differences in national value systems and to technical issues of geolocating 'addresses in cyberspace'. Secure computing

---

[29] See, generally, J Zittrain, *The future of the Internet and how to stop it*, (New Haven Conn.: Yale University Press, 2008).

[30] See Wikipedia, "Trusted Computing" (2012) available at http://en.wikipedia.org/wiki/Trusted_Computing (accessed 28 Oct 2012).

[31] See, e.g., Microsoft, "Sender ID" (2008) available at http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx (accessed 28 Oct 2012).

[32] SW Brenner, "Distributed Security: Moving Away From Reactive Law Enforcement" (2004) *International Journal of Communications Law & Policy*, available at http://ijclp.net/old_website/Cy_2004/pdf/Brenner_ijlcp-paper.pdf (accessed 28 Oct 2012).

may be primarily a technical challenge, but it is intricately interwoven with the distribution of moral responsibilities and legal liability.

The main reason why the dimensions are closely knit, is that regulation, social norms, and technology are not set in stone and do not evolve in isolation. The law, social behaviour, and technology mutually influence each other, in a process of mutual shaping.[33] The law not only steers the development or use of technology, for example by safety product specifications or criminalisation of 'misuse of devices' (as in Art. 6 Cybercrime Convention) – the law also changes due to technological developments, for example when computer-generated child-abuse images are criminalised even though no children have been abused to make them, or when surveillance powers for criminal investigation are broadened through the advent of technologies such as automatic number-plate recognition. Moreover, these changes in law and technology interact with norms and social practices. For example, the 'reasonable expectation of privacy' – a primary yardstick in US Fourth Amendment case-law but also in the application of Art. 8 of the European Convention on Human Rights – partly depends on the extent to which a technology is in use with the general public.[34] The advent of social-networking sites also influences our conception of the public sphere, given the social practice of people publishing on (semi-)open spaces content that is often intended for specific audiences rather than for the general public. This raises questions on what the police can do to automatically monitor open-source spaces in the context of criminal investigations. Can the offline norm of reasonable expectation of privacy based on offline street surveillance be transposed to online surveillance of digital highways, or should we rethink how we conceive of this norm under the influence of what happens on the Internet?

4. Conclusion: The Way Forward for Legal Research

Classic legal research often addresses problems in a rather one-dimensional manner. Frequently, the law is taken as a given and then applied to a societal issue. One can, for instance, argue how harassing someone by creating a fake Facebook profile might be considered a form of stalking and is therefore subject to prosecution on that basis. Sometimes, a social development is taken as a given, and used to argue why and how the law should change. For example, the move from downloading to streaming video in child-porn networks implies that people no longer have child-abuse image in their possession but watch it in real-time online, thereby implying that not only intentional possession, but intentional access to child pornography should be criminalised as well.

However valuable such legal research can be, technology, and the role it plays in the interaction of law and society may provide the often missing link. Technology is shaped by, and at the same time itself shaping, social behaviour and legal and moral

---

[33] Cf. WE Bijker and J Law (eds), *Shaping technology/building society: studies in sociotechnical change*, (Cambridge, Mass.: MIT Press, 1992).

[34] BJ Koops and R Leenes, ""Code" and the Slow Erosion of Privacy" (2005) 12 *Michigan Telecommunications & Technology Law Review* 115-188. For a recent example in Dutch case-law, see District Court 's-Gravenhage 23 December 2011, LJN BU9409, finding that defendant did not have a reasonable expectation of privacy in her backyard as anyone could use Google Earth to see that she had Bubble Cube chairs (the *corpus delicti* of forged tax returns) in her garden.

norms.[35] This implies that technological developments should not be taken for granted when they trigger legal or regulatory questions. Legal research needs to factor in the role that technology increasingly plays in law and society, in the process of the mutual shaping of law, society, and technology.

If criminal law is to stay abreast of the challenges of crime in the 21st century, researchers need a broad perspective on regulation. A thorough dogmatic understanding of the criminal law system itself, focusing on concepts such as *actus reus* or equality of arms, no longer suffices to deal with crime permeated by cyberspace. The advent of organised, money-driven cybercrime that systematically exploits vulnerabilities in the Internet infrastructure to commit cyber-attacks on a global scale requires more complex analyses than merely asking how the cyber-attacks relate to substantive criminal provisions. The affordances of Internet investigations also call for in-depth reflection on the role of criminal investigation in a digitally networked world. We are challenged to rethink the boundaries of criminal investigation itself and to reinvent legal checks and balances in a practice of prevention-driven interventions, where the trial in court can no longer serve as the major touchstone of legal protection.

This implies that criminal law researchers need to be at least as well-versed in regulation theory as they are in criminal law dogmatics. Rather than considering law the only regulatory game in town, researchers should look at all the tools of the regulatory tool-box: besides law, also social norms (such as ethical values or social supervision by capable guardians), market mechanisms (such as business models and pricing mechanisms), and architecture or technology (such as road-bumps or filtering systems) can be used to steer human behaviour.[36] Criminological theories, such as routine activity theory and situational crime prevention,[37] provide additional insights to guide the development of criminal law and legal research in the area of cybercrime.[38] And given the global character of cyberspace, issues of criminal law must be addressed in awareness of the concept and practice of multi-level governance.[39]

Besides familiarity with such elements from regulation theory, the examples of regulatory, normative, and technical challenges also show the need for a multidisciplinary approach. If we aim for prudent solutions to regulatory problems, a purely legal perspective is too narrow. Insights from information science, public policy, Internet sociology, and network economics need to be factored in, if we want

---

[35] WE Bijker and J Law (eds), *Shaping technology/building society: studies in sociotechnical change*, (Cambridge, Mass.: MIT Press, 1992).

[36] See C Raab and P De Hert, "Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood" in R Brownsword and K Yeung (eds) *Regulating Technologies,* (Oxford: Hart, 2008) 263-285 for a discussion of the regulatory tool-box, applying the insights of Lawrence Lessig and Christopher Hood to technology regulation.

[37] M Felson and LE Cohen, "Human Ecology and Crime: A Routine Activity Approach" (1980) 8 *Human Ecology* 389-406; RVG Clarke, *Situational crime prevention: successful case studies*, (New York: Harrow and Heston Publishers, 1992).

[38] See for example NS Van der Meulen, *Financial Identity Theft - Context, Challenges and Countermeasures*, (The Hague: T.M.C. Asser Press, 2011).

[39] L Hooghe and G Marks, "Unraveling the Central State, but How? Types of Multi-level Governance" (2003) 97 *American Political Science Review* 233-243.

to prevent inventing legal solutions that look well on paper but that fail in practice. Ideally, multidisciplinary research should evolve into a truly interdisciplinary undertaking, that is, an approach in which legal, social, and technical theories, practices, and methods are integrated into a unified methodology. Only then are we really equipped to help criminal law find solutions for the problems caused by crime in a globally, digitally networked world.