Enhancing relationships between criminology and cybersecurity

Benoît Dupont
Université de Montréal

Chad Whelan
Deakin University

Cite as:
B. Dupont & Chad Whelan (2021), Enhancing relationships between criminology and cybersecurity, *Journal of Criminology*, DOI: 10.1177/00048658211003925

Abstract
'Cybercrime' is an umbrella concept used by criminologists to refer to traditional crimes that are enhanced via the use of networked technologies (i.e., cyber-enabled crimes) and newer forms of crime that would not exist without networked technologies (i.e., cyber-dependent crimes). Cybersecurity is similarly a very broad concept and diverse field of practice. For computer scientists, the term 'cybersecurity' typically refers to policies, processes and practices undertaken to protect data, networks and systems from unauthorised access. Cybersecurity is used in subnational, national and transnational contexts to capture an increasingly diverse array of threats. Increasingly, *cybercrimes* are presented as threats to *cybersecurity*, which explains why national security institutions are gradually becoming involved in cybercrime control and prevention activities. This paper argues that the fields of cyber-criminology and cybersecurity, which are segregated at the moment, are in much need of greater engagement and cross-fertilisation. We draw on concepts of 'high' and 'low' policing (Brodeur, 2010) to suggest it would be useful to consider 'crime' and 'security' on the same continuum. This continuum has *cybercrime* at one end and *cybersecurity* at the other, with crime being more the domain of 'low' policing while security, as conceptualised in the context of specific cybersecurity projects, falls under the responsibility of 'high' policing institutions. This unifying approach helps us to explore the fuzzy relationship between cyber-*crime* and cyber-*security* and to call for more fruitful alliances between cybercrime and cybersecurity researchers.

Keywords
cybercrime, cyber harms, cybersecurity, criminology, networks, security, security actors

Introduction

Cybercrime and cybersecurity are increasingly being presented among the major social, political and economic challenges of our time. Cybercrime is an umbrella concept used to refer to cyber-enabled crimes (i.e., traditional crimes that are enhanced via the use of networked technologies) and cyber-dependent crimes (i.e., crimes that would not exist without networks technologies; see Wall, 2001 and McGuire and Dowling, 2013). For the most part, criminological research has focused more on cyber-enabled crime and, to a lesser extent, on policing responses to those crimes. Research in this domain is loosely referred to as 'cyber-criminology' (Grabosky, 2016). Cybersecurity is a very broad concept and diverse field of practice. For computer scientists, the term is typically used to refer to policies, processes and practices undertaken to protect data, networks and systems from unauthorised access (Fichtner, 2018; Carley, 2020). It does not matter, from a definitional point of view, whose systems are being considered, with cybersecurity being used in the context of personal devices, the home, workplace and institutions. Rather, the different types and purposes of data, networks and systems are more questions for the precise makeup of cybersecurity. Much like the idea of 'security', cybersecurity is a slippery concept meaning very different things to different people.

The 'securitisation' of cybersecurity cannot be ignored (Kremer, 2014). Indeed, some argue that the term 'cybersecurity' can be understood 'as 'computer security' plus 'securitisation'' (Hansen & Nissenbaum 2009, p. 1160), reflecting the view that shifting from *computer* to *cyber* security shifts from a technical discourse based on protecting systems to a securitising discourse portraying cybersecurity as a specialised domain of national security. An increasingly diverse array of cybersecurity issues are captured under this conceptualisation, including threats posed from espionage emanating from a foreign state, hacking by (state or non-state) terrorists, and various forms of cybercrime. Increasingly, cybercrimes are presented as threats to cybersecurity. Many of the agencies responsible for cybersecurity, particularly signals intelligence agencies, have historically had very little to do with crimes. Interestingly, governments are also potential threats to cybersecurity, as in the cases of protecting personal communications from over-reaching state surveillance. As a field of practice, cybersecurity is concerned largely with the protection of digital infrastructures such as communications, financial and transportation systems (Fichtner, 2018). At the same time, individuals and organisations of all sizes are increasingly being encouraged and responsibilised to practise cybersecurity.

As cyber-criminology and cybersecurity are both concerned with the study of online harms and responses to such harms, it would be logical to assume that these fields share many theoretical and empirical approaches. Upon a closer examination, however, it becomes clear that they are more accurately understood as two discrete academic fields, each mobilising differentiated conceptual frameworks, research questions, datasets, publication outlets and career paths. This paper argues that the concept and field of cybersecurity is in much need of greater conceptualisation. In doing so, we recognise that 'all that we can know about security is what people do in its name' (Valverde, 2011, p. 5), suggesting that efforts should not be caught up in only theorising security but also addressing the practises of security governance. These practises, it is argued, need to be considered in the context of the logics, scale and scope of specific security projects. Our focus in this paper is to consider these questions within the diverse and, at times, contradictory set of actors and practises that make-up the field of cybersecurity.

The paper therefore proceeds as follows. First, we consider in more depth the origins of the cyber-criminology and cybersecurity fields. This allows us to not only further explain the divergence between these cyber fields but also provide insights into how these differences can be better navigated. We therefore hope to promote further integration between these disciplines in future research on cybercrime and cybersecurity. Second, we focus the rest of the paper on the relational dynamics connecting the cyber*crime* and cyber*security* fields, including cyber harms and the actors responsible for preventing and controlling such harms. Drawing on concepts of 'high' and 'low' policing (Brodeur, 2010), we suggest it is useful to consider 'crime' and 'security' on a continuum. This continuum has *crime* at one end and *security* at the other, with crime being more the domain of 'low' policing while security, as conceptualised in the context of cybersecurity projects, is more that of 'high' policing. In the middle of this continuum we see a convergence, where crime and security meet. An increasing amount of cybersecurity problems are occupying this territory, which has significant implications for the cyber field as a whole. We conclude the paper by reflecting on these points of convergence and suggest areas for future research in this field.

Cyber-criminology and cybersecurity

The autonomy maintained by cyber-criminology and cybersecurity as discrete academic fields has resulted in limited engagement between researchers and publications, a situation probably amplified by the technical lineage of cybersecurity within the computer science and engineering disciplines, while cyber-criminology has remained firmly grounded in the social sciences. Hence, one would argue that the logics, spatial and temporal scales, and jurisdictions of concern to cyber-criminology and cybersecurity differ significantly. To understand this surprising disjuncture, it is useful to sketch their scientific genealogies. We will first start with the field of cyber-criminology.

Cybercrime and criminology

The first recorded instances of computers and digital networks being used illegally closely followed their adoption by modern organisations in the 1960s (Parker, 1976). Because computers were bulky mainframes that had not yet been connected to each other, the first generation of cybercrime was mainly the result of insiders abusing their privileged access (Brenner, 2007). The democratisation of personal computers in the 1980s and of the internet in the early 1990s afforded new criminal opportunities to curious and bored adolescents who disrupted digital systems through the development and dissemination of computer viruses and worms, while profit-driven thieves and scammers began to exploit poorly-secured financial transaction systems and to manipulate the trust of internet users (Brenner, 2007; Grabosky, 2016; Lusthaus, 2018). Since then, computer networks, devices, applications and online platforms have shaped every aspect of human activity and have provided a constant stream of new criminal opportunities to innovative offenders.

One of the first issues that criminologists interested in researching cybercrime had to address was to determine where to situate these unfamiliar offenses in the pantheon of traditional crimes usually covered by the discipline. In other words, should cybercrime be treated as a brand-new form of offending, thereby requiring a renewed criminological toolset, or should the hyperbole surrounding its novelty be downplayed to focus on the natural evolution of crime—the "old wine in new bottles" hypothesis (Grabosky, 2001), which could be studied adequately by using conventional theories and methods? One strategy adopted by cyber-criminologists to overcome this dilemma has been to develop inclusive cybercrime typologies that are able to accommodate both well-established crimes supercharged by digital technologies and new

crimes that do not have any historical precedents ('true' cybercrimes). Quite a few variations have been designed over time, but most differentiate between cyber-enabled and cyber-dependent crimes, the former leveraging digital technologies to amplify existing forms of offending (e.g., online fraud or the distribution of child sexual exploitation material), the latter covering malicious activities that would not exist outside of the digital realm (e.g., hacking or denial of service attacks) (McGuire & Dowling, 2013). Others also include cyber-assisted crimes, where digital technologies are incidental to the offense, for example when drug traffickers exchange messages over the internet using encryption tools (Levi et al., 2015; Grabosky, 2016; Wall, 2017). As useful as they are, these typologies accurately reflect patterns of association between humans and machines at a particular point in time but are challenged by the constant changes and new configurations that new technologies introduce and the accelerating pace of this evolution. Just like the term cybercrime overtook the more popular terminology of 'computer crime' in the 2000s to account for the increasingly connected nature of computer systems, one can only wonder how long the concept of cybercrime will maintain its usefulness in a world so saturated by digital technologies that they eventually become invisible to their users (Powell et al. 2018; McGuire, 2020).

The challenge of defining cybercrime has had direct implications on its measurement and the theories that have been mobilised to link it with broader social processes. The ambiguous nature of various cybercrime definitions used over time have impaired the design of statistical tools that could accurately capture its prevalence and measure its impact on society. Existing official crime statistics, on which criminologists traditionally depend, do not adequately reflect cybercrime-specific data. This is because a majority of cybercrimes—and in particular cyber-assisted and cyber-enabled cybercrimes—are prosecuted through statutes that pay more heed to the substance of the offence than to the technological means used to commit the crime. A growing share of crimes also incorporate online and offline components, making cybercrime harder to disentangle from local street crime (Levi, 2017; Roks et al., 2020). As a result, the recording of such offences in most countries still remains problematic or fragmented (Lavorgna, 2020, p. 20), and only raw estimates of the global costs of cybercrime can be made (McGuire, 2018). This leaves criminologists at the mercy of cybersecurity firms and think-tanks that produce dubious surveys and statistics as marketing material, often grossly exaggerating the prevalence of cybercrime and the financial harm it causes (Florêncio et al., 2014).

Empirically, criminologists have greatly benefited from the behavioural visibility of cyber-offenders (Leonardi and Treem, 2020), whose activities can be followed with relative ease on online convergence settings such as hacking forums and illicit marketplaces (Pastrana et al., 2018; Rossy & Décary-Hétu, 2018). This has allowed them to explore market forces at work, including the role played by trust, reputation, social ties, expert knowledge, business practises, and operational security measures—to name a few—in the criminal performance of these underground markets, and of their participants (Holt, 2017). A smaller number of studies have also relied on youth surveys to understand the onset of pathways to cybercrime (Fox & Holt, 2020; Brewer et al., 2018), as well as to compare cyber-offenders with traditional offenders (Weulen Kranenbarg et al., 2019). A few researchers have also managed to interview malicious hackers and to gain access to police investigative files (Leukfeldt et al., 2017; Lusthaus, 2018), opening a window into the offending patterns, thinking models and rationalisation processes of cyber-offenders. In parallel, the experience of cybercrime victims has attracted significantly less attention, with studies trying to understand susceptibility to cybercrime victimhood and to better document the unmet needs of cybercrime victims (Button & Cross, 2017; Leukfeldt et al., 2020). Finally, more attention is being paid to the attitudes, capacities and effectiveness of law

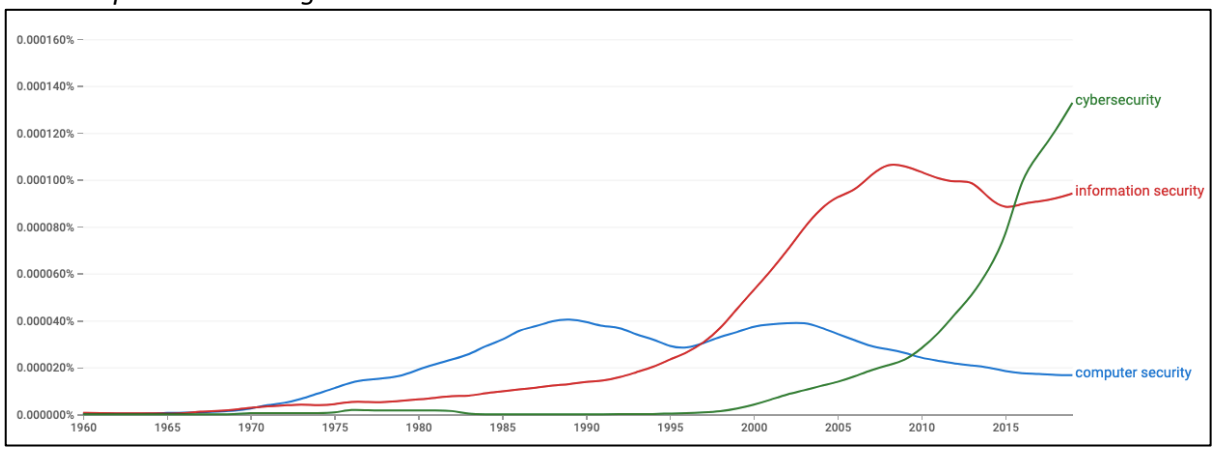
enforcement organisations (Holt & Bossler, 2012; Harkin et al. 2018) and the civilians supporting them (Whelan and Harkin 2019).

Most cybercrime publications rely on existing criminological theoretical frameworks, trying to assess their compatibility with a fast-digitising society. Classical theories such as deterrence theory, routine activity theory, general strain theory, social learning theory, differential association theory, the general theory of crime or drift theory remain dominant as explanatory factors in the cybercrime literature (Bossler, 2020). By contrast, publications that leverage science and technology studies' frameworks such as actor-network theory (van der Wagen & Pieters, 2020), or that examine more thoroughly the co-evolution of specific technologies and criminal innovations (McGuire, 2008; Wall, 2017; Dupont, 2020) are still comparatively rare. Because of the technical skills required, empirical evaluations of interventions seeking to disrupt or prevent cybercrime activities are extremely scarce (Collier et al., 2019; Maimon & Louderback, 2019), and when they exist, they are not always able to capture the contribution of public-private linkages and partnerships enabling such interventions (Dupont, 2017). This difficulty to account for the dispersed nature of cybercrime control and prevention capacities and responsibilities is mirrored by cybersecurity's limited engagement with criminological insights.

Cybersecurity: from national security to behavioural perspectives

While it may not have reached the status of a full-fledged discipline yet, cybersecurity as a research field is quickly developing at the intersection of computer science, political science and 41 other disciplines (Carley, 2020). Like their cyber-criminologist colleagues, cybersecurity researchers have also seen shifts in the terminology used to frame their research agenda, from computer security in the 1960s to information security in the 2000s, the cyber- prefix gaining widespread acceptance in the 2010s (Landwehr, 2010). The Google Books Ngram graph below displays the occurrence frequency of the three terms in the 40 million books scanned by Google and published in English between 1960 and 2019. This evolution does not merely reflect new trends launched by scientists eager to differentiate their work from their predecessors'. It also denotes the broadening focus of cybersecurity, which expanded beyond its initial narrow interest in the security of machines to gradually incorporate considerations about the information stored and processed by these machines, and ultimately the humans and social institutions interacting with both.

Figure 1: Occurrences of the terms 'cybersecurity', 'information security' and 'computer security' in books published in English between 1960 and 2019



Source: https://books.google.com/ngrams

The fields of computer science and engineering account for 70-80% of cybersecurity publications, while social science research comes a distant second with 18-30% of publications, depending on which bibliographic database is queried (Dunn Cavelty, 2018; Dhawan et al., 2020). The computer science and engineering strands of cybersecurity research are primarily focused on hardware and software vulnerabilities, with limited concerns for the 'manufactured' nature of those risks, which are enabled by IT companies favouring innovation and speed of growth over security, and are exploited by human adversaries who never stop to innovate. Aware of this shortcoming, a growing number of computer scientists rely on human-computer interaction theories and leverage behavioural economics to provide more accurate explanations of the cyber-risk landscape and to design more effective interventions (Moore, 2010; Briggs et al., 2017).

Ever since its precursor technologies were developed in the late 1960s with seed funding from the United States Defence Department's Advanced Research Project Agency, the internet has been closely associated with military interests (Castells, 2002). The internet's military heritage partly explains why cybersecurity is predominantly framed as a national security issue by political scientists (Dunn Cavelty, 2018). This mindset implies that online risks are construed as existential threats to the survival of the polity, requiring exceptional responses from intelligence and defence institutions to address the most unimaginable (and often 'hyped') catastrophic scenarios (Kremer, 2014). Securitising online harms is problematic, because such emergency responses may be used to justify the violation of legal and social norms (Hansen & Nissenbaum, 2009), while failing to properly acknowledge the negative financial and emotional consequences suffered by millions of cybercrime victims.

Empirically, and by contrast with cyber-criminologists, cybersecurity researchers have used their technical clout to develop a broader range of measurement strategies to assess the contours of the cyber-threat landscape, the risk exposure of various organisational actors, the harm suffered, and the effectiveness of the security measures put in place. Using diverse data sources such as criminal forum posts, insurance prices, stock market activity, bitcoin transactions, legal cases, data breach incident reports, and surveys collected and processed automatically using customised computer programs and algorithms, they have debunked some myths, such as the out-of-control nature of cybercrime (Woods and Böhme, 2020). However, because of the disciplinary background of the researchers driving these methodological efforts, the technical breakthroughs that enable the collection, processing and visualisation of vast quantities of hard-to-access data often receive more attention than the social and policy insights these data can generate. Very few of these datasets are available to criminologists, with some notable exceptions, such as the data sharing framework implemented by Cambridge's Cybercrime Centre (Pastrana et al., 2018).

Thus, despite the growing attractiveness of cybersecurity to many established disciplines, it is still dominated by computer scientists and engineers, and to a lesser extent by political scientists. This lack of transdisciplinary engagement seems counterproductive, both for cybersecurity (which misses out on insights on crime prevention, deterrence, social network analysis of criminal enterprises, third party policing, or victimisation, to name a few) and for cyber-criminology (which remains partially blind to the contributions automated analytical tools such as machine learning and deep learning algorithms can make to the detection and categorisation of crime patterns, or to the crime control and prevention capacities deployed by private and non-governmental actors). In that context, we believe it is time to end this

separation of technical, political and criminological knowledge (Dunn Cavelty, 2018: 26), which only fragments our capacity to make sense of online harms in a world where law enforcement and national security institutions, on the contrary, seem to converge in a reconfiguration of the security field.

Appreciating the relational dynamics of the cyber field

Intersecting cyber-harms

The varied cyber-related harms are the focus of many institutional actors comprising this broad security field. Our objective is not to describe such actors, which would constitute a monolithic mapping exercise, but rather to highlight the relational attributes among them. Various attempts to categorise cybercrime and cybersecurity threats and harms have been put forward (e.g., de Bruijne et al., 2017; Agrafiotis et al., 2018). However, any such attempt is a starting point rather than an end in itself, as it helps to frame the distribution of responsibilities and capacities within the cyber field.

Australia's most recent *Cyber Security Strategy* groups cyber-threats into four categories: financially motivated criminals, issue or politically motivated actors, terrorist and extremists, and state sponsored actors or nation-states (Australian Government, 2020). It is common to view the first two examples more in relation to cyber-*crime* and the subsequent two in relation to cyber-*security*. However, this basic characterisation hides much complexity and obfuscates the growing overlap between different types of cyber-risks. For example, while some financially motivated criminals may be fairly low-level in relation to their sophistication and victim impacts, the potential exists for such actors to target large scale financial institutions causing systemic economic harms (Bouveret, 2018). Issue or politically motivated groups may similarly range from seeking to promote a political message through to more significant risks or harms that could potentially challenge conceptions of national security (e.g., financial stability). Some such threats may be caused by individual actors (the proverbial teen hacker operating from his or her parents' basement), whereas others may result from groups of actors whose scope extends from local gangs to national or transnational networks.

Finally, new threat configurations erasing the convenient boundaries that characterise existing typologies emerge on a regular basis. For example, the leaks of offensive hacking tools developed by the National Security Agency and the Central Intelligence Agency (probably orchestrated by intelligence adversaries) have been exploited by for-profit hackers to fuel their cybercrime spree, effectively using American intelligence agencies as their Research and Development laboratories (Trend Micro, 2019). Cyber-attackers working on behalf of nation states have also been observed selling access to the networks they infiltrated for espionage purposes to cybercriminals and running ransomware campaigns to increase their profits (Group IB, 2020), while in a symmetrical hybridisation process, state-sponsored groups are buying access to targets of interest from cybercrime groups (GReAT, 2020). Where cyber-related harms and their associated security actors sit along the 'low' and 'high' policing (Brodeur, 2010) continuum is therefore difficult to tease apart.

New cybersecurity actors

It is therefore not surprising that this security field includes a diverse array of actors that cross long-established organisational boundaries, including policing, intelligence, and defence agencies along with policy departments from multiple levels of government. Some of these actors have much more experience and expertise to respond to cyber harms than others. Police,

for example, are widely known to struggle to deal with cybercrime, while signals intelligence agencies have developed deep expertise in cybersecurity and have received very generous funding as a result of their central role in national cybersecurity strategies.

Over the last five years in particular, most governments have established new organisational forms in an effort to bring many diverse capabilities together. The Australian Cyber Security Centre (ACSC), established as a standalone agency within the Australian Signals Directorate (ASD), includes staff from five government agencies in law enforcement, criminal intelligence, security intelligence, signals intelligence and defence sectors. Computer Emergency Response Teams, among others, located in policy areas of government were also relocated into the ACSC at the time. The ACSC's purpose is to provide a hub for information-sharing and public and private sector collaboration on cyber security, including preventing and responding to cyber threats and harms. It is similar to the National Cyber Security Centre (NCSC) in the United Kingdom (UK), established in October 2016, and the Canadian Centre for Cyber Security (CCCS), established shortly after Australia's in 2018, each also part of their respective signals' intelligence agencies. In all cases, such centres report to cooperate with private stakeholders though there is no formal membership status extended outside of state actors. Alongside these centres, many governments have directed significant resources to funding centres specialising in cybersecurity research and commercialisation.[1]

There are some notable differences between countries that we would like to reflect on a little here. For example, the activities of the ACSC are potentially broader than their equivalents in the UK and Canada. As mentioned above, it has a core function in relation to the reporting of cybercrimes, previously the responsibility of the Australian Criminal Intelligence Commission (ACIC).[2] When making a report, complainants are asked to identify as a person or individual, business or organisation, or government department. If reporting as an individual, the overwhelming majority of such reports are likely to be cybercrimes. Those making reports are informed that their matter will be passed onto the relevant police service and may or may not be investigated. In these cases, reports to the ACSC are likely for information gathering purposes only. There are no state police, who are responsible for most cybercrimes against individuals, in the ACSC and each state jurisdiction manages cybercrime reports in different ways. The UK, in contrast, has multi-agency Regional Organised Crime Units (ROCUs) that are hosted by the National Crime Agency (NCA), have responsibility for cybercrime and are connected to the NCSC. The commitment to similar units in Australia has been affirmed (Australian Government, 2020); however, the focus of the Joint Cyber Security Centres in Australia is more about engagement with cybersecurity stakeholders (amongst other things), including in the private sector, and less about responding to cybercrime. The NCSC is not responsible for the UK public online reporting tool, *Action Fraud*, which is instead overseen by the National Fraud Intelligence Bureau. Although clearly not all cybercrimes can be considered fraud, these represent the majority involving the public whereas breaches of cybersecurity are varied. As part of Canada's National Cyber Security Strategy (Public Safety Canada, 2018), the Royal Canadian Mounted Police was awarded significant funding to create a National Cybercrime Coordination Unit, with the mandate to coordinate and provide investigative advice to local police organisations, liaise with national security and international partners, and launch a national public reporting mechanism for individuals and businesses (Public Safety Canada, 2019). Thus, in both the UK and Canadian case, increased investment and multiagency responses are evolving in relation to *both* cybercrime and cybersecurity, whereas in Australia this is much more so in field of cybersecurity. Even in the context of cybersecurity, furthermore, while strong national networks

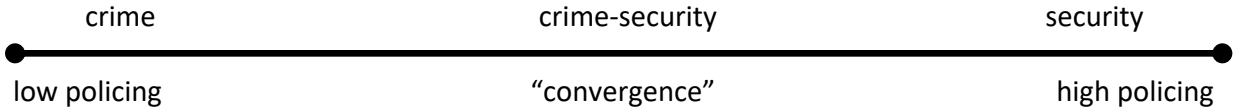
have been established to connect different security actors (Whelan & Dupont, 2017), how well these connect at the subnational level is unclear.

Since the formation of the ACSC, the two most recent Director-Generals of the ASD have given become much more public as the activities of such agencies become increasingly promoted. The same general principle is true across the Five Eyes community as cyber-related harms have brought about greater visibility to this domain of high policing. As such, signals intelligence agencies, not long ago largely hidden from public view, are now taking a much more prominent position in the cybersecurity field. This role extends to advising business on cybersecurity resilience and practical steps for individuals to improve their cyber safety at home. The ACSC has engaged in continual campaigns and other strategies in a deliberate effort to raise its profile, largely with a goal of enhancing cybersecurity awareness and thus preventing online harms. Indeed, the Australian Security Intelligence Organisation (ASIO) has similarly just launched its first public campaign called 'think before you link', equally focused on raising awareness around cyber security (ASIO, 2020). The activities of such actors, however, are legally defined and differentiated. While the ACSC is within ASD, it is quite distinct from other ASD roles, which are exclusively focused offshore, including offensive cyber capabilities. While ASIO, as a security agency, is largely domestically focused, its national security and counterintelligence mandate is different from conventional crime. ASD has recently publicly revealed its role in offensive cyber operations in disrupting terrorist groups, and in the last year has reportedly directed its capabilities against foreign cyber criminals behind COVID-19 themed phishing campaigns targeting Australian residents (Australian Government, 2020).

Blurring boundaries across the crime-security continuum

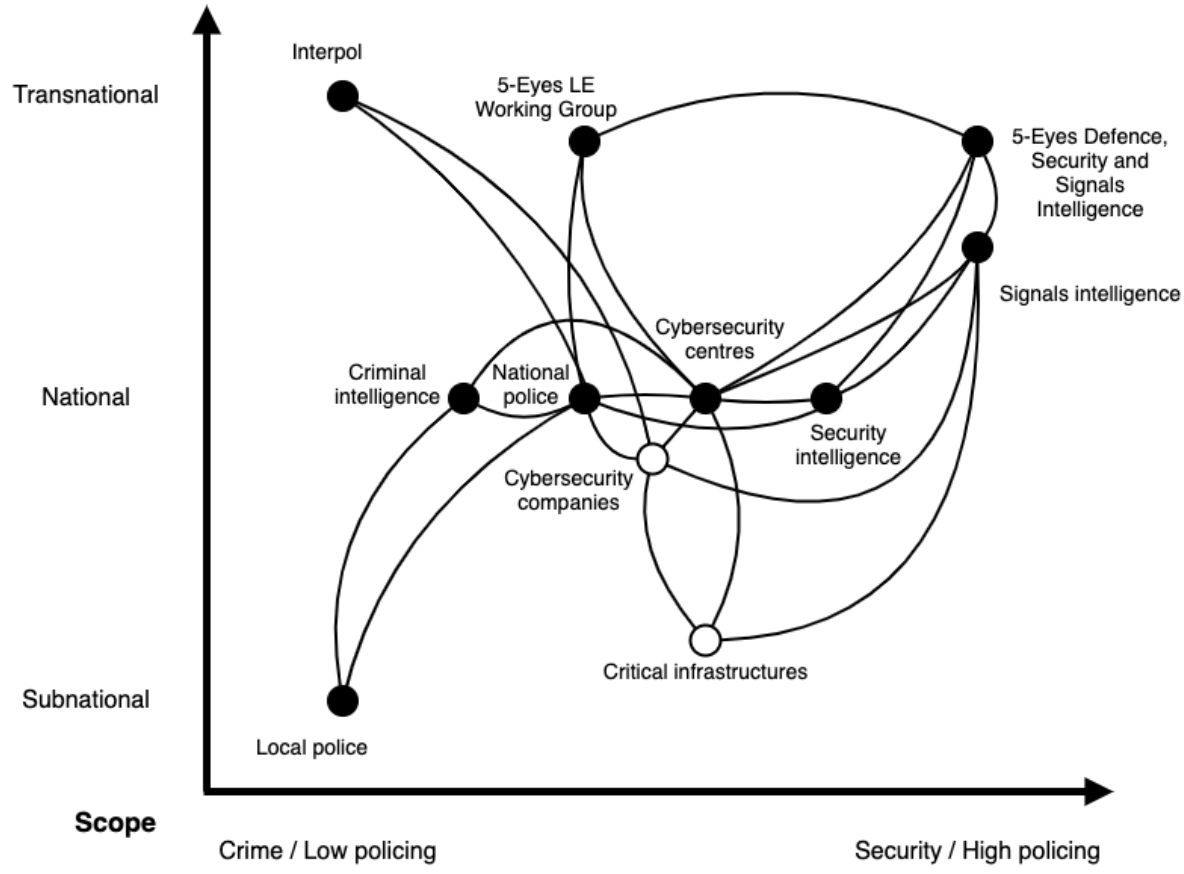
These boundaries are further blurring, however. For example, recent debate has occurred in relation to the potential for ASD to play a role in offensive cyber capabilities against transnational crime networks such as those involved in child sex offences and people smuggling (Australian Broadcasting Corporation, 19 February 2020). Many of these activities have long been the responsibility of the Australian Federal Police (AFP), the key federal agency investigating and prosecuting such offences. Although it is a legal requirement of most signals intelligence agencies across the Five Eyes that they cannot collect intelligence within their national borders, many have provisions to allow them to assist other actors such as national police or security intelligence agencies where that is requested. These examples serve to highlight our underlying argument that there are multiple points of convergence where cybercrimes and threats to cybersecurity meet. These developments are not unique to Australia. In 2015, the UK established a co-located Joint Operations Cell involving a collaboration between the Government Communications Headquarters (GCHQ) and the NCA (GCHQ, 2015). While this cell was initially focused exclusively on disrupting online child sexual exploitation, the relationship has since extended to many types of serious and organised crime, including fraud, money laundering, people trafficking, and various forms of illicit smuggling activity. We therefore see high policing agencies becoming increasingly involved in low (or lower) policing activities.

Figure 2: crime-security continuum



The idea of a crime-security continuum is one way to begin to address the complexity of the cyber field. We situate crime at the 'low' policing end with security at the 'high' policing end. What becomes clear from doing so, if it was not clear from the paper already, is the many points of convergence we see in the middle (see Figure 2). For example, in one detailed review of cyber threat actor typologies, the authors identify 11 threat actor ideal-types: extortionists, information brokers, crime facilitators, digital robbers, scammers and fraudsters, crackers, insiders, terrorists, hacktivists, state actors, and state-sponsored networks (de Bruijne et al., 2017). These actors are then differentiated by their expertise, resources, organisational form, and motivation. Although some of these actors could be viewed as being exclusively cybersecurity threats (e.g., state actors and state-sponsored networks), it is not quite as simple to do the same in relation to cybercrime. As mentioned above, financially motivated criminals might engage in activities that can clearly be viewed as crime, but the same actors could also direct their activities against higher risk targets (such as critical infrastructures) or be enrolled by state actors to conduct espionage campaigns or cyberattacks. In other cases, as in the examples of child sex exploitation, it is not the activity itself that elevates something from a crime problem to a security problem but rather the level of difficulty that capacity-limited police services experience in responding to such activities. An increasing amount of such harms therefore gets pushed into the middle of the crime-security continuum, if not much closer to security. The security actors comprising the cyber field are thus inextricably connected (see Figure 3 for a high-level overview that simply aims to demonstrate some potential ties between cyber actors, with black dots representing state actors and white dots private actors).

Figure 3: the cybersecurity field



In addition to mapping out the cyber field, the crime-security continuum has normative implications. There are cyber harms that we argue belong firmly in the low and high domains

specifically. This is not to say anything about their seriousness insofar as victim impacts. In contrast, we argue that some harms are better recognised as crime problems rather than security problems, and that their corresponding security actors should focus on different harms based on where they sit along this continuum. In particular, we would argue there is a much greater need for police–especially local police–to become involved in the cyber field. Some activities, most notably fraud and scams against individuals or organisations, are indeed criminal activities and we argue should be the focus of police (the difficulty in obtaining successful prosecutions notwithstanding). Even illicit activities undertaken by child sex syndicates and transnational crime groups would normally be considered *crime* and not threats to *security* (although they clearly are significant harms and threats to the security of individuals – but this is also the case if such activities were undertaken in physical environments). In Australia, many of these activities are the focus of relatively small specialist units whereas in other contexts, there are more resourced multi-agency settings (e.g., the ROCUs). Mapping this out also necessitates that a deeper set of questions be considered, such as what areas of cybercrime should be the focus of local police compared with national police, police rather than intelligence, intelligence rather than defence, how international organisations such as Interpol should be involved, and so on. This requires a much more developed and nuanced assessment of the cyber field, as well as a more thorough debate on the governance and accountability issues such arrangements raise.

Conclusion

This paper is a starting point in seeking to promote much greater collaboration between and among disciplines in approaching the field of cybercrime and cybersecurity. It has highlighted how these fields emerged as discrete research problems and argued that much greater integration is needed to further advance these research fields. We have argued that both cybercrime and cybersecurity have been constrained by this bifurcation, meaning each would benefit from input from the other. Our primary goal has been to examine the relationships between cybercrime and cybersecurity, and to reflect on what this relationship means for conceptualising this particular security field. Ultimately, it may be that all we have been able to successfully do is highlight what a challenging endeavour this will prove. Much like the term 'security' (e.g., Zedner, 2009), we need to recognise that cybersecurity means different things to different people. Different conceptions of security have emerged as an effort to denote specific security threats and referent objects. For example, distinctions are made between ideas such as 'human security', 'national security' and 'international security'. If cybersecurity is viewed as a specialist domain of national security (which it clearly is, for some), we should not be surprised that political scientists focus on its securitisation. But it is clear that cybersecurity is about more than national security. Indeed, in the case of cybersecurity, there is an enormous potential of referent objects, ranging from individuals, organisations and corporations of all sizes, through to nation states and even international networks of state and non-state actors. It may be time to think deeply about whether additional pre-fixes to the term 'cybersecurity' would indeed add clarity to this field. The longstanding distinction between 'low' and 'high' policing (Brodeur, 2010) may have some utility at the extremes, with 'low cybersecurity' relating to such things as routine internet security and protecting personal accounts and devices, while 'high cybersecurity' includes protecting government systems against computer intrusions from state actors. Between these two extremes, there are many harms that can be classified in varying ways.

The difficulties in neatly defining cyber-related harms are also evidenced in the responses of governments and security actors. The introduction of new network-based cybersecurity centres undoubtedly has a number of positives in relation to both promoting cybersecurity awareness

as well as harnessing resources to respond to cyber threats across organisational boundaries and professional disciplines. Yet, when we look at the growing number of harms that are captured under the banner of 'cybersecurity', and the increasingly diverse focus of such centres, it is clear that one cannot evoke the term cybersecurity and expect the audience to appreciate its intended meaning. The same term has dramatically different implications if it is being evoked in the context of local or personal devices and systems compared with those of financial institutions or the apparatus of government. Even within government, furthermore, the term has very different implications if we are focusing on protected to highly classified information such as in defence contexts.

Definitions aside, the cybersecurity field is converging along new configurations that blur the lines between law enforcement and national security, low and high policing, public and private security. We should question whether it is in fact desirable or not for traditional high policing agents (signals intelligence agencies) to have such a public role in cybersecurity, particularly in relation to cybercrime problems that are definitely more *crime* than *security*. For example, this could exacerbate the status of certain types of cyber threats, perhaps even unnecessarily, while other threats may not be given the attention they deserve because the cybersecurity field is becoming increasingly 'crowded' with a growing volume of harms. More specifically, elevating responses to cybersecurity without intentionally doing the same for cybercrime risks insufficient policy attention being directed on cybercrime as it becomes conflated with–or absorbed by–cybersecurity. This is particularly likely as sophisticated attacks such as the recently reported SolarWinds hack against the US supply chain become increasingly high profile. There are, as such, a number of reasons as to why the relationships between cybercrime and cybersecurity are in critical need of added scrutiny. As much as we would like to be able to provide more direction with regard to how these many challenges could be navigated, we too are deeply reflecting on these very developments. We hope to stimulate further interdisciplinary research and policy innovation in this field.

Notes

[1] Examples of such centres include the Cyber Security Cooperative Research Centre in Australia, which received $50 million in Commonwealth funding over seven years in 2018.

[2] The ACIC was responsible for coordinating the Australian Cybercrime Online Reporting Network (ACORN), which was a national cyber-crime reporting tool. Reports could be made from any jurisdiction in Australia and cases were assigned to the respective state or territory police. An evaluation of ACORN was conducted in 2016 but not released publicly until August 2018 (see Morgan et al. 2016). Many criticisms of ACORN were raised and the decision to remove this separate reporting function and conflate it with the activities of the ACSC was reportedly partly a response to these. The new reporting tool was introduced in 2019.

References

Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1-15. https://doi.org/10.1093/cybsec/tyy006

Australian Broadcasting Corporation (2020). Government considering bringing foreign cyber spy powers onshore to hunt Australian paedophiles. 19 February 2020. <https://www.abc.net.au/news/2020-02-19/powers-for-asd-spy-dark-web-australians/11980728> last accessed 20 January 2021.

Australian Government (2020). *Australia's Cyber Security Strategy 2020*. Commonwealth of Australia.

Australian Security Intelligence Organisation. (2020). *Think before you link*. <https://www.asio.gov.au/TBYL.html> last accessed 20 January 2021.

Bossler, A. (2020). Contributions of criminological theory to the understanding of cybercrime offending and victimization. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 389-407). Routledge.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Brenner, S. (2007). History of computer crime. In K. de Leeuw & J. Bergstra (Eds.), *The history of information security: A comprehensive handbook* (pp. 705-721). Elsevier.

Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young people, the internet, and emerging pathways into criminality: A study of Australian adolescents. *International Journal of Cyber Criminology*, *12*(1), 115-132. http://doi.org/10.5281/zenodo.1467853

Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In L. Little, E., Sillence, & Joinson, A. (Eds.), *Behavior change research and theory* (pp. 115-136). Academic Press.

Brodeur, J.-P. (2010). *The policing web*. London: Oxford University Press.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.

Carley, K. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365-381. https://doi.org/10.1007/s10588-020-09322-9

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society*. Cambridge University Press.

Collier, B., Thomas, D., Clayton, R., & Hutchings, A. (2019). *Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks.* IMC '19: Proceeding of the Internet Measurement Conference, Amsterdam. https://doi.org/10.1145/3355369.3355592

De Bruijne, M., van Eeten, M., Gañán, C., & Pieters, W. (2017). *Towards a new cyber threat actor typology: A hybrid method for the NCSC cyber security assessment.* Delft University of Technology.

Dhawan, S.M., Gupta, B.M., & Elango, B. (2010). Global cyber security research output (1998-2019): A scientometric analysis. *Science & Technology Library*. https://doi.org/10.1080/0194262X.2020.1840487

Dunn Cavelty, M. (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, *6*(2), 22-30. http://dx.doi.org/10.17645/pag.v6i2.1385

Dupont, B. (2013). Skills and trust: A tour inside the hard drives of computer hackers. In C. Morselli (Ed.), *Illicit networks* (pp. 195-217). Routledge.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change*, *67*(1), 97-116. https://doi.org/10.1007/s10611-016-9649-z

Dupont, B. (2020). The ecology of cybercrime. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 389-407). Routledge.

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, 7(2), 1-19. DOI: 10.14763/2018.2.788

Florêncio, D., Herley, C., & Shostack, A. (2014). FUD: A plea for intolerance. *Communications of the ACM*, *57*(6), 31-33. https://dl.acm.org/doi/pdf/10.1145/2602323

Fox, B., & Holt, T. (2020). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854820969754

Government Communications HeadQuarters. (2015). *GCHQ and NCA join forces to ensure no hiding place online for criminals*. 6 November 2015. <https://www.gchq.gov.uk/news/gchq-and-nca-join-forces-ensure-no-hiding-place-online-criminals> last accessed 20 January 2021.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243-249. https://doi.org/10.1177/a017405

Grabosky, P. (2016). *Cybercrime*. Oxford University Press.

GReAT (Global Research & Analysis Team) (2020, November 19). *Advanced threat predictions for 2021*. Kaspersky Secure List Blog. https://securelist.com/apt-predictions-for-2021/99387/

Group IB (2020). *Hi-tech crime trends 2020-2021*. Group IB.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155-1175. http://www.jstor.org/stable/27735139

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, *19*(6), 519-536. https://doi.org/10.1080/15614263.2018.1507889

Holt, T., & Bossler, A. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking*, *15*(9), 464-472. https://doi.org/10.1089/cyber.2011.0625

Holt, T. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime*, *18*(1), 1-10. https://doi.org/10.1080/17440572.2016.1235821

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law*, *23*(3), 220-237.

Landwehr, C. (2010). *History of US Government investments in cybersecurity research: A personal perspective*. 2010 IEEE Symposium on Security and Privacy, Oakland. https://doi.org/10.1109/SP.2010.41

Lavorgna, A. (2020). *Cybercrimes: Critical issues in a global context*. Red Globe Press.

Leonardi, P., & Treem, J. (2020). Behavioral visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, *41*(12), 1601-1625. https://doi.org/10.1177/0170840620970728

Leukfeldt, R., Notté, R., & Malsch, M. (2020). Exploring the needs of victims of cyberdependent and cyber-enabled crimes. *Victims & Offenders*, *15*(1), 60-77. https://doi.org/10.1080/15564886.2019.1672229

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, *61*(11), 1387-1402. https://doi.org/10.1177/0002764217734267

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2015). *The implications of economic cybercrime for policing*. City of London Corporation.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

Maimon, D., & Louderback, E. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*, 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

McGuire, M. (2008). *Hypercrime: The new geometry of harm*. Routledge.

McGuire, M. (2018). *Into the web of profit: Understanding the growth of the cybercrime economy*. Bromium.

McGuire, M. (2020). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In R. Leukfeldt & T. Holt (Eds.), *The human factor of cybercrime* (pp. 3-28). Routledge.

McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Morgan, A. et al. (2016). *Evaluation of the Australian Cybercrime Online Reporting Network*. Canberra: Australian Institute of Criminology.

Parker, D. (1976). *Crime by computer*. Charles Scribner's Sons.

Pastrana, S., Thomas, D., Hutchings, A., & Clayton, R. (2018). *CrimeBB: Enabling cybercrime research on underground forums at scale*. WWW 2018: The 2018 Web Conference, Lyon. https://doi.org/10.1145/3178876.3186178

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. London: Routledge.

Public Safety Canada (2018). *National cyber security strategy: Canada's vision for security and prosperity in the digital age.* Public Safety Canada.

Public Safety Canada (2019). *National Cyber Security Action Plan 2019-2024*. Public Safety Canada.

Roks, S., Leukfeldt, R., & Densley, J. (2020). The hybridization of street offending in the Netherlands. *The British Journal of Criminology*, azaa091. https://doi.org/10.1093/bjc/azaa091

Rossy, Q., & Décary-Hétu, D. (2018). Internet traces and the analysis of online illicit markets. In Q. Rossy, D. Décary-Hétu, O. Delémont, & M. Mulone (Eds.), The Routledge international handbook of forensic intelligence and criminology (pp. 249-263). Routledge.

Trend Micro (2019, October 18). *Putting the eternal in EternalBlue: Mapping the use of the infamous exploit*. Trend Micro Blog. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/putting-the-eternal-in-eternalblue-mapping-the-use-of-the-infamous-exploit

Valverde, M. (2011). Questions of security: A framework for research. *Theoretical Criminology*, *15*(1), 3-22. https://doi.org/10.1177/1362480610382569

Van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, *17*(4), 480-497. https://doi.org/10.1177/1477370818812016

Wall, D. (2001). Cybercrimes and the Internet. In D. Wall (Ed.), *Crime and the Internet* (pp. 1-17). Routledge.

Wall, D. (2017). Towards a conceptualisation of cloud (cyber) crime. In T. Tryfonas (Ed.), *Human aspects of information security, privacy and trust* (pp. 529-538). Springer.

Weulen Kranenbarg, M., Ruiter, S., & Van Gelder, J.-L. (2019). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*. https://doi.org/10.1177/1477370819849677

Whelan, C., & Dupont, B. (2017). Taking stock of networks across the security field: A review, typology and research agenda. *Policing and Society*, *27*(6), 671-687. https://doi.org/10.1080/10439463.2017.1356297

Whelan, C. & Harkin, D. (2019). Civilianising specialist units: Reflections on the policing of cyber-crime. *Criminology and Criminal Justice*. https://doi.org/10.1177%2F1748895819874866

Woods, D., & Böhme, R. (2020). *Systematization of knowledge: Quantifying cyber risk*. 42nd IEEE Symposium on Security and Privacy. Oakland.

Zedner, L. (2009). *Security.* London: Routledge.