Reference: CU 2021/10(B)/DTA/OCB/CSS

Comments in response to the **Compilation of all preliminary conclusions and recommendations suggested by Member States during the meetings of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in 2018, 2019 and 2020** (UNODC/CCPCJ/EG.4/2021/CRP.1).

Prepared by
Dr Matthew Sorell,
Senior Lecturer, Digital Forensic Science
School of Electrical and Electronic Engineering
matthew.sorell@adelaide.edu.au

Associate Professor Tim Legrand,
Associate Professor,International Security
Department of Politics and International Relations
tim.legrand@adelaide.edu.au

31 March 2021.

Detailed comments

The distinction between cybercrime, cyber-enabled crime, and physical crime with associated digital evidence

At II.A.5(f) (page 5/23), fifteen cyber-related acts are itemised in the context of criminalisation, and at II.A.5(g) a comment is made that "computer-specific offences are drafted as tailor-made provisions that do not simply extend the application of traditional offences to the digital environment…"

The relevance of this recommendation is to harmonise expectations that computer-specific offences committed at a distance, and in particular from within the jurisdiction of one state but with the target (person, information or cyber-physical system) potentially within another state or states, can be investigated and prosecuted within the state of origin.

As observers of the meeting since 2013, we welcome the enumeration of specific forms of crime which might be considered as cybercrime, but we note almost immediately the conflict with II.A.5(g), since these paragraphs together conflate the three concepts of cybercrime, cyber-enabled crime, and cyber-evidence. This point is touched on at IV.A.8(a) where the distinction is made between cybercrime and cyber-enabled crime but the implications of this distinction are not followed through.

In reviewing this list, we identify the following distinctions:

i. Facilitating cyber-enabled crime through the provision of platforms, services or expertise.
ii. The theft of intellectual property and the infringement of copyright, through hacking into systems or through fraud and deception.
iii. The use of the Internet, potentially across borders, to commit acts related to terrorism, and to incite hate crime and violent extremism.
iv. Intercepting data, and damaging or negatively impacting data, computer systems and critical information infrastructure, which may include the exploitation of the ever-growing diverse range of connected devices ("Internet of Things") to deploy botnets and distributed denial of service attacks, through to the specific targeting and disruption of critical physical infrastructure through cyber means, such as shipping, power generation and distribution, banking, and government services.
v. Financial crimes related to fraud, financial theft, anonymous or pseudonymous financial transactions, and crimes which exploit obfuscation of identity and the incapacity of authorities in other states to respond in a timely manner. Such crimes include theft, scams, blackmail, ransomware, tax evasion, the distribution of child exploitation material, and the trade of illegal or restricted goods such as people, drugs, weapons and wildlife.
vi. Crimes against the person such as the disclosure of personal information or "revenge pornography", the market for child sexual abuse and exploitation material, and the incitement of minors to commit suicide.

The above list has been ordered to show a continuum from crimes that are most closely associated with crimes committed within "cyberspace" (that is, from a remote location, on the internet, predominantly exploiting Internet-connected infrastructure, at global scale and unprecedented speed, and impersonal in its reach) through to those which are predominantly real-world crimes of infrastructure damage, financial gain, and crimes against the person, which are facilitated by the characteristics of "cyberspace" (that is, from a distance, with enhanced anonymity, communicated over the Internet, predominantly exploiting Internet-connected real-world infrastructure, at global scale and unprecedented speed, impersonally targeting people and markets).

The core issue from a criminalization perspective is the potential to commit an offence at a distance, by means of electronic communication, and in particular targeting systems, information or persons outside the state of origin.

We draw the distinction between "cybercrime" and "cyber-enabled crime" to make the point that in the latter case the issue of criminality becomes less contentious, and the core criminalization in a cybercrime context is to provide some clarity around inter-State cooperation and recognition of "action at a distance". Conversely, we make the point that "cybercrime" is a term that encompasses criminalization of acts which are identified as offences committed at a distance but with more tenuous links to real-world targets or victims.

Observation 1: the harmonised criminalization of certain cybercrime acts facilitates investigation and prosecution of offences committed at a distance over the Internet, noting that while dual criminality is usually required for extradition it is not a necessary requirement for mutual legal assistance.

To this list, we add real-world crimes for which there is little if any "cybercrime" element, but for which the same issues of cross-border cooperation in relation to evidence and investigation of digital evidence apply. Of particular relevance is telecommunications, social network posts, geolocation data, health data and other data and metadata collected from a diverse range of connected devices and processed and stored in cloud servers. One author (Sorell) has extensive experience assisting law enforcement agencies investigating major crime and serious and organised crime, involving digital evidence sourced from outside the home jurisdiction.

Of critical relevance is timely access to evidence. There are three perspectives here. The first is to gain access to ephemeral digital records before they expire or are deleted. The second is evidence to respond to a real or perceived immediate threat to life. The third is the emergency response to shut down public access to certain content – a specific example being the Christchurch mosque shootings on 15 March 2019, which was livestreamed by the perpetrator on Facebook.

Observation 2: investigations requiring cooperation between States to access, contain or control digital evidence include not only offences committed at a distance, but also evidence that is retained outside the encapsulated jurisdiction of the offence.

The final observation is that evidence may be stored, duplicated, or distributed across multiple servers in multiple jurisdictions by a private entity. Having established a hypothetical process for assistance from the private entity through, for example, an established point of contact in one jurisdiction, can that private entity then obstruct access to data which is held by its servers in a different jurisdiction? And is there a further role for intergovernmental cooperation to manage such obstruction?

The challenge on the one hand is to ensure that there is agreement on the circumstances under which interjurisdictional cooperation to access, contain, or control evidence can operate; and on the other to ensure that there mechanisms in place to do so which are timely, effective, reasonable, proportionate, and which balance a lawful request for assistance with due process guarantees, privacy interests, civil liberties and human rights (at 5(b) page 4/23), taking into account the urgency of the request for assistance.

Observation 3: digital evidence associated with cybercrime, cyber-enabled crime and associated with physical world crime is commonly held by private organizations which may operate in multiple States. The emerging challenge is not just cooperation between states, but cooperation between a state and a private sector organisation which may offer services in the state's jurisdiction but which may not have a registered office or staff within the state. Further, there are myriad examples of such private sector organizations which set out to protect the private data of their customers by design, and in some cases promote that they do so in order to deliberately protect customer data from investigation.

Technology neutrality, standard processes, and criminal innovation

At II.A.4(a) (page 2/23) the point is made that "legislative provisions [should] withstand the test of time with regard to future developments in technology by enacting laws with formulations that are technologically neutral and criminalize the activity deemed illegal instead of the means used", a point also raised at III.A.6(j) (page 7/23) and III.B.7(a)(v) (page 9/23).

This is problematic for several reasons. Firstly, the emphasis is on describing the crime and limiting the scope of consideration to "cybercrime", when, we argue, the more relevant matter is ensuring timely and balanced access to digital evidence through mutual legal assistance.

Technology neutrality is therefore applicable to the process of access, containment and control of digital evidence, rather than to whether or not a codified criminal offence has been committed.

This does not dissuade from the potential need to criminalise activity which is expressly "cybercrime" (occurring wholly or predominantly in relation to computers) or the cyber characteristics of cyber-facilitated crimes (those relating, for example, to terrorism, financial crimes, disruption of infrastructure, crimes against the person), and this is especially important if a criminal threshold needs to be met before interjurisdictional cooperation can be activated.

The evolution of cyber-related crime is twofold.

Firstly, technology continues to develop in its complexity and capability. As bandwidth, processing power, system architectures and innovative new products come online, the capability of law enforcement and investigative agencies to access, contain and control digital evidence is increasingly put under strain.

Observation 4: technologically neutral language is needed in cooperation agreements to ensure that new innovations in cyber technology and services remain in scope.

Secondly, criminals innovate within the capabilities of the digital communications technologies to which they have access and the circumstances in which they find themselves. The deployment of "deep fake" video for example has enabled a new form of revenge pornography, and the impact of SARS Covid-19 on office workers being sent home to work under quarantine or lockdown has dramatically increased the attack surface for cyberattacks against infrastructure, companies and individuals.

In this regard, technological neutrality is not the issue. Rather, it is recognising that crime evolves, and can sometimes do so in disruptive ways.

For example, is the production and dissemination of synthetic "deep fake" video as "revenge pornography", child abuse material, incitement to terrorism or misleading public disinformation defined as a crime?

Another example is fraud perpetrated through online shopping channels. A compelling advertisement is shown in social media (a fake designer handbag). A payment of less than $50 is made. A package arrives in due course, but instead of the purchased item, an almost worthless item (a packet of seeds, a rayon scarf) is supplied, along with a receipt for an item worth perhaps $1000. The purpose of the fraud is to create a paper trail to facilitate money laundering. The victim is unlikely to report being duped, and if they do report, the amount lost is unlikely to result in an inter-jurisdictional investigation. This is a cyber-facilitated financial fraud, but the specificity of the facilitating technology is largely irrelevant.

These examples note that not only will criminals exploit new technologies to find new ways to pursue their objectives, an overly prescriptive definition of crimes and procedures create gaps and loopholes which are the focus of exploitation.

Observation 5: technologically neutral language in both criminalization of cyber-related crimes and in cooperation agreements is needed in order to address criminal innovation in a a rapidly evolving cyber environment.

At IV.A.(8)(j) (page 14/23), it is noted that "[t]here is a need to prepare an internationally acceptable standard operating procedure regarding the collection and preservation of data that can be followed at the scene of a crime. Universal adoption of standard international practices on the collection, storage and sharing of evidence are critical, in particular in the process of investigation of cybercrime and prosecution of cybercriminals"

Similarly at IV.A.(8)(lll) (page 19/23), it is noted that "[t]he international community should formulate a unified procedure for cybercrime investigation techniques and improve regulations on the log preservation of Internet service providers in their domestic laws"

These paragraphs are problematic, because they take as their starting point an assumption that digital evidence is static in its nature, and indeed that there is a definable "scene of a crime". They are, in other words, recommendations that run counter to both technology neutrality and crime neutrality.

On the other hand, at IV.A.(8)(g), it is noted that "[s]tates should consider the creation of innovative protocols for the exchange of information…" - a different point than technical procedures but with similar challenges. It needs to be very clear that innovation runs the risk of ad hoc procedures which may not meet legal requirements. But innovation is necessary, which necessitates a clearly defined set of principles.

In the ten years of the Expert group, mobile phone networks have migrated from second generation technology, through third and fourth generations to the emerging fifth generation. The assumptions that underpinned the operation, and therefore the records, of second generation telephony were disrupted by the emergence of data services in the third generation, shaken again by the evolution of core network technologies from circuit switched to packet (Internet protocol) technologies as the fourth generation rolled out, and are now facing the challenge of complex virtual private network and privacy preserving features in the fifth generation. The prescriptive procedures for mobile telecommunications records, alone, are falling behind the network capabilities, even though large scale mobile network technology standards are known years in advance.

In that time we have also seen the emergence of wearable devices processing personal biometric data in cloud services in near real time, the increasing dominance of social media as a platform for communication, the abuse of private data for political gain, and the introduction and rise of cryptocurrencies.

Looking forward, we are now seeing the early stages of the autonomous vehicle market with its inherent cybersecurity challenges, the launch of a global satellite internet communications network which potentially bypasses ground-based interception points, the widespread application of artificial intelligence and machine learning, the potential development of quantum computing at a commercial scale, and a global vaccination effort in response to a global pandemic which is an enormous attack surface for fraud, theft and disinformation in cyberspace.

To get some idea of how much the cyber world will change in the next ten years, we need only look back to see how much it has changed over the last decade. And then scale for exponential growth.

Observation 6: In order to meet the recommendations for standard procedures, it is necessary that these be properly formulated on principles rather than prescription, recognise technological neutrality and deliberately accommodate flexibility as new sources

of online digital ("cyber") capabilities and evidence and new forms of criminal activity become evident. To do otherwise is to leave gaps and loopholes for criminal exploitation.

We make the point that just as cultural norms are not uniform across Member States, neither should it be assumed that evidence logged by machines developed and maintained in different jurisdictions follow uniform technical protocols. In practice, systems log data according to the assumptions of the engineers that initiated the product, driven by the requirements of the vendor and the end customer, tempered by local regulation and maintained with a view to ongoing profitable operation.

This adds a further layer of complexity to the notion of standard procedures, because there also then needs to be an additional stage of scientific validation of forensic evidence if those logs are to be accepted by the Court.

Implicit in the conclusion and recommendations is the notion that evidence can in fact be accessed, identified, secured, acquired, decrypted or decoded, and transmitted.

Observation 7: The challenges presented by the form and function of digital evidence are an active focus of technical research and forensic validation. This is not a static research area because the scale and scope of cyber technologies and related criminal activity continues to grow exponentially in volume and complexity.

Research and the Role of Academia
At A(6)(q) (page 8/23) relevant reference is made to Academia "with a view to enhancing knowledge and strengthening the effectiveness of responses to cybercrime".

There are also three references to "research", each of which has a clear academic context but there is no explicit linkage to academic research.

Two other references are made to academia in the context of education around "prevention" of cybercrime. In our view, this under-values the role of academia in understanding, responding to, and strengthening the responses to crime which is committed in cyberspace, facilitated through cyberspace, or which leaves digital evidence in cyberspace.

We encourage the Expert Group to consider how to harness multi-disciplinary research to better meet the objectives of the report. This might include, for example, providing a portal to relevant academic research, support of relevant multi-disciplinary conferences, and other means of supporting the commissioning and dissemination of research. If that research is visible to member states, it offers new opportunities to understand new and emerging criminal threats linked to cyber space.

Translational Research and Capacity Building
We highlight for example the need for translational research that bridges the gap between legislative objectives, law enforcement capabilities, and the technical behaviour of cyber-enabled systems which are often not designed for forensic analysis (and in some cases are deliberately designed to thwart the acquisition and analysis of forensic evidence).

We also highlight the important role of academic in developing and facilitating capacity building projects, including applied and translational research and the dissemination of that research not only in the context of sovereign capability but also to share knowledge and resources with the wider international community.

At a policy-making level, there is a clear need for research on identifying best-practices in transgovernmental cooperation to counter cyber crime and related pathologies. It is widely recognised that establishing reciprocal data-sharing and threat-sharing information between national law enforcement agencies, with built-in protections for human rights, is a growing imperative to prevent criminal networks' exploitation of the cross-boundary gaps in law enforcement. Emerging research on transgovernmental law enforcement (e.g. Saskia Hufnagel; Tim Legrand; Christian Leuprecht) is highlighting how multilateral agreements can speed cross-border collaboration and close these enforcement gaps.

Transgovernmental enforcement networks of policing agencies, such as those active between Australia, Canada, New Zealand, the UK and US, are already demonstrating how data-exchange can proceed on the basis of Memoranda of Understanding, rather than formal treaties, while not contravening domestic law and the legal authorities of the respective agencies. Identifying the mechanisms in place that work effectively, and those that do not, will require collaborative research between academics and those agencies.

Dr Matthew Sorell

Dr Matthew Sorell is Senior Lecturer in telecommunications and multimedia engineering in the School of Electrical and Electronic Engineering at the University of Adelaide. He specialises in digital forensic science and has extensive operational experience working closely with law enforcement agencies in Australia and around the world.

His policy experience in Australia includes reports on cyber vulnerabilities of small form factor satellites (2019); Technology trends (2014, Australian Crime Commission); Privacy, security and identity management implications of cloud computing for home users and small to medium enterprises (2010 for the Department of Broadband, Communications and the Digital Economy); New and Emerging Technologies in the context of content classification (2005-2006, for the Office of Film and Literature Classification); and Media streaming (2002).

Dr Sorell has also reviewed and advised on telecommunications and banking sector applications for the Australian Research and Development Tax Incentive for the Australian Department of Industry and Innovation.

Dr Sorell was appointed Adjunct Professor of Digital Forensics at the Tallinn University of Technology, Estonia, in 2018, where he teaches and supervises students in matters relating to digital evidence, forensics and criminal investigation.

He also delivers a private consulting service to law enforcement and related agencies in Australia, and has provided operational advice to a range of international agencies, most notably in the UK and the United States.

In 2018 he received a High Commendation for developing emerging sources of digital investigation at the International Digital Investigations Awards in London, for his work on wearable devices.

Dr Sorell is an academic member of the INTERPOL Digital Forensics Experts Group. He has attended the UNODC Intergovernmental Experts Group on Cybercrime as an academic observer since 2013; and is Scientific Adviser to FORMOBILE, an EU Horizon 2020 research project addressing mobile phone evidence from crime scene to court room. In 2022 he will chair the DFRWS APAC (Digital Forensic Research Workshop – Asia Pacific) conference in Adelaide.

Dr Sorell is chair of the SA Node Advisory Board of AustCyber, leads cyber education collaboration between the University of Adelaide and the Tallinn University of Technology (Estonia), and has received a Citation for Excellence in Teaching from the Australian Learning and Teaching Council (2009).

Associate Professor Tim Legrand

Associate Professor Tim Legrand joined the Department of Politics and International Relations in July 2018. He has previously held research and lecturing positions in the National Security College at the Australian National University, the ARC Centre of Excellence in Policing and Security at Griffith University, and also held visiting research fellowships at the Institut d'Études Politiques de Paris (Sciences Po), Johns Hopkins University, the University of East Anglia and The University of Stockholm. His PhD in Political Science, funded by the Economic and Social Research Council, was awarded by the University of Birmingham in 2008.

Tim is adjunct Associate Professor of Public Policy at the Centre for Governance and Policy Analysis at the University of Canberra, Co-Convenor of the APSA Policy Studies Research Group, and is the former Secretary-Treasurer of the Australian Political Studies Association.

Tim's research is concerned with national and international dimensions of global security decision–making, particularly in transnational networks and institutions.

His work traverses a range of security themes, principally in global blacklisting and sanctions, cyber security and critical infrastructure, terrorism, political violence and political exclusion. This research is distinctive in its cross-pollination of public administration (law, sociology and public policy) literatures and International Relations (critical security studies, global governance) perspectives to navigate the complex terrain of security in domestic and international spaces. He is the author or editor of five books, including *The Architecture of Policy Transfer: The Power of Ideas, Institutions and Networks in Transnational Policymaking* (2021, Palgrave Macmillan) and *Banning them, Securing us? The Politics of Proscription*, with Lee Jarvis. (2020, Manchester University Press).

Professor Legrand engages widely with governments, NGOs and IGOs. His work of proscription and blacklisting has been used in the International Court of Justice in The Hague, and by the Swiss Refugee Council and United Nations. Within Australia, in 2013 he was appointed as an expert advisor to an Inquiry by the Commonwealth Inspector of Transport Security on aviation and maritime security. He has presented his research to the Department of Foreign Affairs & Trade, The Department of Home Affairs, Department of Defence, Australian Federal Police and Prime Minister & Cabinet. Within Australia, his work has also formed the basis of submissions to a Queensland Parliamentary committee, the COAG Review of Counter-Terrorism Legislation (2012) and the Commonwealth Independent National Security Legislation Monitor. In the UK, he has worked or engaged with the Home Office and Foreign & Commonwealth Office, the Departments of Health and Communities and Local Government.

Professor Legrand has been awarded more than $1m in research funding in the past three years. His funded projects all have the same imperative: to accurately identify emerging global security dilemmas and find resolutions or mechanisms to mitigate their impacts. The outcomes of this research feed directly into enhancing policy and practice for national governments, NGOs and International Organisations.

The University of Adelaide

The University of Adelaide is a global leader in research, innovation and teaching. We discover new knowledge to better the world and prepare the leaders of tomorrow. Our University is amongst the elite universities in the world, ranking consistently in the top 1% of the world's universities.

The best and brightest

We recognise exceptional people are our greatest asset, and invest significant resources in making our university a global destination of choice for the very best minds. Among our distinguished alumni we have five Nobel Laureates; over 100 Rhodes Scholars, including Australia's first Indigenous recipient; and Australia's first female prime minister and Supreme Court judge. We attract a diverse student body of over 27,000 from more than 90 countries. Bright young minds learn alongside internationally recognised leaders in their fields, developing research skills, an innovation mindset, an international perspective and career readiness.

Translatable research excellence

A strong commitment to research excellence has defined the University of Adelaide's history. We are South Australia's sole member of the Group of Eight, Australia's research-intensive universities. Our researchers are committed to solving the world's grandest challenges. We are equally proud of the fact that 100% of our research sub-fields are rated 'world standard or above' by the Australian Research Council's Excellence in Research Australia program. The University's specialist institutes and centres bring together world-leading researchers, partner with industry and government, supported by modern infrastructure and an innovative culture, to tackle state and national research priorities. We strive to build an ever-stronger nexus between our research and local economic needs, leveraging creativity and knowledge to create abundant economic opportunities. We continually enhance links between research and education to help shape a new generation of entrepreneurs able to translate new knowledge into societal benefit.

Global perspective

Our reputation and rankings make us an attractive partner for many of the world's most prestigious higher education institutions, research centres, global firms and government agencies. Connection to global knowledge through partnerships brings tangible outcomes, including welcoming world-leading experts to Adelaide to share their knowledge with peers, the expansion of our research capabilities through cross-institutional teams, access to global competitive sources of funding, the acquisition of resources from international consortia, the sharing of complementary infrastructure, and a flow of new people, new ideas and new processes to enrich our State. We aspire to be part of a global exchange of knowledge, learning, business engagement and investment opportunities, beneficial to our community.