CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

PJCLE SUBMISSION: The capability of law enforcement to respond to cybercrime

cybersecuritycrc.org.au

To whom it may concern,

Submission: Parliamentary Joint Committee on Law Enforcement – The capability of law enforcement to respond to cybercrime

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Law Enforcement's inquiry into the capability of law enforcement to respond to cybercrime.

Cybercrimes are a significant and increasing issue for law enforcement. They are also among some of the most complex crimes law enforcement is required to deal with, largely due to the borderless nature of the internet.

With digital connectivity increasing, and its centrality to the lives of Australians and the effective operation of our institutions and organisations becoming more ubiquitous, it is important effective policies are in place to support law enforcement. Key to this is the development of a clear understanding of the scope and scale of the issue and supporting the community to better comprehend what cybercrime is and how they can protect themselves from new and emerging digital threats.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem.

We look forward to answering any queries about this submission and welcome the opportunity to participate in any future consultation.

This submission has been prepared by CSCRC management. The CSCRC Board was not involved in the preparation or drafting of this submission.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre

Introduction

Cybercrimes are a significant and increasing issue for law enforcement. They are also among some of the most complex crimes law enforcement is required to investigate and prosecute, largely due to the borderless nature of the internet and the technical aspects of cyber security.

With digital connectivity increasing, and its centrality to the effective operation of our institutions, infrastructures and organisations becoming more ubiquitous, it is important effective policies are in place to support law enforcement to fight cybercrime. Key to achieving this is developing a better understanding of the scope and scale of cybercrime, enhancing community understanding of what cybercrime is and mitigations against victimisation, and economy-wide coordination to help detect and prevent cyber threats.

Australian law enforcement works hard to keep the community safe from all crime, including cybercrime. However, unlike more 'traditional' offences that occur in the physical realm, cybercrimes are often viewed as 'intangible', which means they continue to be under-reported. Furthermore, given the speed at which technology continues to evolve, cybercrime is not static, with new exploits and tactics constantly being developed and deployed.

In Australia, law enforcement agencies are best placed to provide information and advice regarding operational matters, including capabilities and coordination in relation to cybercrime. Therefore, this submission focuses less on operational issues and more on the definition of cybercrime, how it is measured and offender and victim characteristics.

It also examines key challenges law enforcement faces in the detection, investigation and prosecution of cybercrime, namely extraterritoriality, encryption technologies and cryptocurrencies.

Finally, the submission addresses emerging threats that should be considered, specifically the impacts artificial intelligence (AI) and IoT cybersecurity could have on cybercrime.

Defining 'cybercrime'

Defining cybercrime is difficult given its breadth and mutability, making it a topic of considerable academic debate.[1]

The Australian Federal Police (AFP) defines 'cybercrime' as: "crimes directed at computers or other information communications technologies (ICTs), such as computer intrusions and denial of service attacks; crimes where computers or ICTs are an integral part of an offence, such as online fraud".[2]

Given the dynamic and evolving nature of cybercrime, the Cyber Security Cooperative Research Centre (CSCRC) supports this two-pronged definition, which encapsulates cyber-dependent and cyber-enabled crimes. The key distinction between these two methods of cybercrime is the role of ICT – whether it is the target of an offence or used as a means through which to commit a crime.[3]

[1] Defining Cybercrime | SpringerLink
[2] Cybercrime | Australian Federal Police (afp.gov.au)
[3] Cybercrime Key Issues: Cybercrime in Brief (unodc.org)

While taking a two-pronged definitional approach is important, the CSCRC submits there is scope to further articulate 'cybercrime' in a way that prevents digital dualism. This may assist in making them more 'tangible' and serve to reduce shame and stigma associated with cybercrime victimisation.

The notion of 'digital dualism' views the digital and physical realms as separate spheres and fails to recognise the effects one domain may have on the other, an approach that can be pervasive in relation to cybercrime.[4] It operates upon the assumption that the real-world social interactions of individuals do not impact their online behaviour and propensity to commit or become a victim of cybercrime, and vice versa. However, research indicates otherwise, with Luekfeldt et al finding core members of cybercrime groups often held offline connections before establishing online social relationships, which were strengthened and reinforced online.[5] Similarly, offending that often begins online, like grooming of minors, can escalate into 'real life' contact offending.[6]

A factor that is important to denote, which is also supported by research, is that in online environments individuals do not experience the same behavioural inhibitions as in off-line contexts. As a result, "online offenders are psychologically, socially and physically further removed from their offences and victims, encounter fewer and/or less severe consequences for their behaviours and are likely to repeat these offences, emboldened by their experience".[7]

By taking a holistic approach and ensuring digital/physical divides are broken down in relation to cybercrime, it can be defined in a way the community can better understand in relation to its forms and impacts.

Cybercrime and the legislative framework

Australia's criminal offence and law enforcement framework to address cybercrime is strong, captured across a range of offences under the *Commonwealth Criminal Code Act 1995*.

These offences include:

- dishonestly obtaining or dealing in personal financial information
- online child sexual exploitation and abuse
- cyber abuse including non-consensual sharing of intimate images
- computer intrusions
- unauthorised modification of data, including destruction of data
- unauthorised impairment of electronic communications, including denial of service attacks
- the creation and distribution of malicious software (for example, viruses and ransomware).[8]

In addition, states and territories have their own cybercrime related offences and legislation that deals with online fraud and other technology-enabled crimes.[9]

[4] View of Beyond Cybercrime: New Perspectives on Crime, Harm and Digital Technologies (crimejusticejournal.com)
[5] The Use of Online Crime Markets by Cybercriminal Networks: A View From Within - Rutger Leukfeldt, Edward Kleemans, Wouter Stol, 2017 (sagepub.com)
[6] Experiences in Online Grooming from Initial Contact with Offender to Relationship Ending (waldenu.edu)
[7] Understanding cybercrime in 'real world' policing and law enforcement - Joanna Curtis, Gavin Oxburgh, 2023 (sagepub.com)
[8] Cybercrime | Attorney-General's Department (ag.gov.au)
[9] Ibid.

Both the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and Surveillance Legislation Amendment (Intercept and Disrupt) Act 2021* have supported the investigation of cybercrime in Australia. Through these laws, the AFP, Australian Crime and Intelligence Commission (ACIC) and other law enforcement-related agencies have expanded powers to collect intelligence, conduct investigations, disrupt and prosecute serious criminal online activity. Such powers are vital in countering serious cybercrime.

While the framework is strong, there is a need to consistently review the utility of Australian law as it relates to cybercrime to ensure it remains fit-for-purpose in a rapidly evolving environment. While encryption technologies remain a significant hurdle for law enforcement in the detection and investigation of cybercrime, emerging technologies, notable generative artificial intelligence, must be more thoroughly considered now and into the future.

Motivations of cybercriminals

Cybercriminals are not homogenous – they can be individuals, groups, state-sponsored actors and nation states. And because of this diversity, they have varying motives and intent for committing cybercrimes.

Individuals and organised groups generally commit cybercrimes for personal gratification or financial gain, for example, through phishing scams, ransomware attacks or the proliferation of online child abuse material (CAM).

State-sponsored actors and nation states, on the other hand, are more likely to partake in disruption, espionage or foreign interference activities like, for example, disruption of critical infrastructure, intellectual property theft and information operations (disinformation campaigns).

Hacktivist groups have also become increasingly active due to global conflicts, notably in the Ukraine and Middle East, with cybercrimes committed to further a particular political, ideological or social cause.[10]

What are the characteristics of cybercriminals?

While there is no 'typical' cybercriminal', research from the University of Bristol has highlighted specific characteristics associated with individual offenders.[11] They found cybercriminals are more likely to be males in their late teens and twenties, have a greater likelihood of completing a higher level of education and greater academic competence, spend a greater amount of time on the internet, and are more likely to be employed in computing and technology occupations or be unemployed.[12]

Among cybercriminals, research indicates there is a perception that the risk of being caught is relatively low.[13] This is the often the result of a 'disassociation' from offending due the anonymity

[10] Escalation of Threats in the Middle East | CyberPeace Institute
[11] Characterising Cybercriminals: A Review (arxiv.org)
[12] Ibid
[13] Understanding cybercrime in 'real world' policing and law enforcement - Joanna Curtis, Gavin Oxburgh, 2023 (sagepub.com)

afforded by the internet, reduced inhibitions, and a decreased sense of proximity to victims, which reduces feelings of guilt and fear of retaliation.[14]

Through developing a better understanding of the characteristics of cybercriminals, diversionary programs can be better developed and implemented. There is evidence from both the UK and the Netherlands of the success of such diversionary programs, especially for young people.

In the UK, the Metropolitan Police have developed a program called Cyber Choices, targeting individuals who may be vulnerable to committing cybercrime and diverting them onto a more productive path by using educational visits, workshops and online training.[15]

Following this model, Dutch law enforcement developed a program called Hack_Right, which is aimed at preventing cybercrime recidivism. Working with industry partners, the program has been successful in discouraging cybercrime and encouraging young offenders to move to legal activity, such as ethical hacking.[16]

Who is most at risk of cybercrime victimisation?

According to the Australian Institute of Criminology's (AIC) *Cybercrime in Australia 2023* report, younger people are more likely to be cybercrime victims than older people in Australia.[17]

The report, which used a representative sample of 13,887 Australians, found almost 31% of respondents aged 18-24 years reported being a victim of a malware attack in the 12 months prior to the survey. The next highest age group to fall victim were those aged between 25-34 years (24.4%), with the age groups least likely to fall victim those 65 years and older (20.3%) and 50-64 years (18.5%).[18]

The reason for higher victimisation of young people correlates with more time spent online. According to the report, more frequent social media use was associated with significantly higher rates of cybercrime victimisation and, among respondents who were able to estimate the time they spent online, the longer they spent online for personal use, the more likely they were to be a victim of cybercrime.[19]

Re-victimisation was common among the cohort, as was victimisation across multiple forms of cybercrime. Researchers found that while 26.5% of respondents were a victim of one type of cybercrime, 20.1% of respondents (43.1% of all victims) were victims of two or more types of cybercrime in the 12 months prior to the survey.[20]

In terms of organisational victimisation, small to medium business owners, operators and managers experienced much higher rates of all types of cybercrime. Respondents who worked for a large business or company, on the other hand, were less likely to have been victimised.[21]

[14] Understanding cybercrime in 'real world' policing and law enforcement - Joanna Curtis, Gavin Oxburgh, 2023 (sagepub.com)
[15] Cyber Choices | Metropolitan Police
[16] Hack_Right: Dutch cybercrime prevention program comes of age | The Daily Swig
[17] Cybercrime in Australia 2023 (aic.gov.au)
[18] Ibid
[19] Ibid
[20] Ibid
[21] Ibid

Unfortunately, researchers found most cybercrime victimisation went unreported to police or to ReportCyber, which mean official statistics significantly underestimate the size of the problem.[22] This effect, known as the 'dark figure' of cybercrime, is not a problem isolated to Australia – it is a global trend.[23]

According to Queensland University of Technology's A/Professor Cassandra Cross, underreporting is the result of multiple factors including, but not limited to, "not knowing who to report to, a belief that nothing can be done, the shame and embarrassment about being victimised, and the cross-jurisdictional nature of most cybercrime offences".[24] A/P Cross also states that enhancing victim support mechanisms could serve to increase cybercrime reporting by reducing stigma and shame associated with victimisation, but notes that delivery of support services through law enforcement would not be the most appropriate model.[25]

Measuring the cost of cybercrime

Measuring cybercrime and its cost, both economic and social, is difficult due to underreporting, as highlighted above.[26] However, domestic and global statistics indicate that rates of cybercrime continue to increase year-on-year, as do the costs.[27][28] Domestically, it is estimated cybercrime cost about $33 billion in 2020-21 and globally it is estimated to cost between USD$100 billion to USD$6 trillion annually.[29][30]

Cybercrime trend research recently released by the NSW Bureau of Crime Statistics and Research (BOCSAR), showed a 42% increase in cybercrime in NSW in the three years to June 2022.[31] During this period, cyber-fraud increased by 95% and identity crime increased by 35%. Device offences (malware and ransomware) had the largest increase, with reports up by 117%.[32]

As highlighted in the Australian Signals Directorate's (ASD) *Annual Cyber Threat Report 2022-23*, Australia's most populous states report more cybercrime, with Queensland and Victoria recording disproportionately higher rates of cybercrime relative to their populations.[33]

Federal and jurisdictional coordination

While this submission does not address operational law enforcement mechanics in relation to federal and jurisdictional cybercrime, the CSCRC would like to note the hard work that has been undertaken to enhance the effectiveness and efficiency of coordination efforts. This is the case domestically, with the AFP leading coordination with state and territory police forces, and internationally, with the AFP embedding officers in international jurisdictions and supporting

[22] Cybercrime in Australia 2023 (aic.gov.au)
[23] Understanding cybercrime in 'real world' policing and law enforcement - Joanna Curtis, Gavin Oxburgh, 2023 (sagepub.com)
[24] Dr Cassandra Cross submission (homeaffairs.gov.au)
[25] Ibid
[26] 2022 National Plan to Combat Cybercrime (homeaffairs.gov.au)
[27] ASD Cyber Threat Report 2022-2023 | Cyber.gov.au
[28] Why we need global rules to crack down on cybercrime | World Economic Forum (weforum.org)
[29] 2022 National Plan to Combat Cybercrime (homeaffairs.gov.au)
[30] OECD work on digital security policy
[31] Trends in and characteristics of cybercrime in NSW
[32] Ibid
[33] ASD Cyber Threat Report 2022-2023 | Cyber.gov.au

overseas operations. Such coordination has led to many successful cybercrime convictions and has helped boost regional law enforcement responses to cybercrime.

A shining example of successful coordination is the AFP-led Joint Policing Cybercrime Coordination Centre (JPC3), which targets high-harm and high-volume cybercrime in Australia. Located in Sydney, the JPC3 brings together representatives from the AFP and all state and territory forces, Five Eyes counterparts, major regulators and the big four banks. Co-located, these representatives can share real-time threat intelligence and work collaboratively to investigate and prosecute cybercrimes.

The CSCRC submits that, given the success of the JPC3 model, there is scope to expand its further enhance its operations. This would not only serve to enhance cybercrime expertise across Australian law enforcement, it would support 'breaking down siloes' to ensure more efficient and effective law enforcement mechanisms for the Australian community.

Key challenges

Given the borderless nature of the internet, law enforcement faces complex and evolving challenges in fighting cybercrime. While these challenges are myriad, this submission focuses on three key challenges facing law enforcement in the detection, investigation and prosecution of cybercrimes. These are extraterritoriality, encryption and cryptocurrency.

Extraterritoriality

Cybercrime challenges the orthodox notions of state, transcending borders and traditional notions of 'territoriality'. This has significant implications for the detection, investigation and prosecution of cybercrime. A central challenge in relation to extraterritoriality is the impunity particular jurisdictions provide to cyber criminals, who are essentially permitted to offend without legal ramifications. This has been especially marked in relation to ransomware syndicates run out of eastern Europe. As a result, the chances of bringing offenders located in these jurisdictions before Australian courts is low.

In such a challenging environment, international collaboration is essential for law enforcement. Two key initiatives being spearheaded by Australian law enforcement to help overcome challenges associated with extraterritoriality are highlighted below.

The Australian Centre to Counter Child Exploitation (ACCCE)

Led by the AFP, the ACCCE brings together key stakeholders and partners to drive a collective effort to counter the child exploitation. Applying an integrated and collaborative model, it harnesses the expertise of federal, state and territory, non-government agencies and private industry, allowing a "cross-pollination" of resources, knowledge and skillsets between stakeholders.[34]

The ACCCE works closely with other law enforcement agencies across the world and focuses on countering online child sexual exploitation, including organised child exploitation networks

[34] ACCCE Overview Sept 2022

operating in the online environment.[35] In 2022-23, the ACCCE's work resulted in 120 children being removed from harm, 186 arrests and 925 charges being laid.[36]

The International Counter Ransomware Taskforce (ICTRF)

The ICRTF, which was established in 2023 and chaired by Australia, is an international collaboration of 37 nations to strengthen international efforts to combat ransomware and help build global resilience against malicious cyber actors.

The work of the ICTRF is involves and complements the work of the 100-person joint AFP and ASD operational grouping, which works to actively disrupt the activities of cybercriminals.[37]

Encryption

Encryption technologies, especially those associated with online messaging applications and the dark web, present a significant barrier to the detection, investigation and prosecution of cybercrime.

In a recent statement, the ACCCE noted the challenge encryption posed for law enforcement, warning "the proposed widespread implementation of end-to-end encryption by major technology and social media companies will make it harder to identify illegal communications or data transmitted through those platforms".[38]

Encryption is the conversion of information or data into unintelligible code, which prevents unauthorised access. While it provides a key role in keeping personal and valuable information protected, it is also widely used by criminals to cloak their illicit activities. Encryption makes it difficult for law enforcement to intercept and read messages criminals send each other and to trace cryptocurrency increasingly used to fund criminal enterprise.

End-to-end encryption provides a form of communication protection that prevents third parties – including internet service providers, app hosts and law enforcement – from accessing data transferred from one system or device to another. This means data is encrypted on one system or device and only the recipient can decrypt it. Encrypted instant messaging apps use end-to-end encryption to ensure only the person a message is sent to is able to access it, meaning a third-party intercepting the messages cannot read them, as they will be indecipherable.

These services operate 'over the top' of traditional telephony networks, which means it is impossible to know when they are even being used. Examples of well-known encrypted instant messaging apps include Signal, Telegram and WhatsApp.[39]

The dark web is not like the surface web, the external interface of the internet most people are familiar with. It is part of the internet that evades indexing by search engines, instead requiring the use of an anonymising browser (like Tor) that routes traffic through multiple servers, encrypting it along the way.

[35] ACCCE Overview Sept 2022
[36] ACCCE achievements 22-23.pdf
[37] Counter Ransomware Initiative (homeaffairs.gov.au)
[38] AFP and US strengthen partnership to combat child abuse | Australian Federal Police
[39] CSCRC Submission - PJCLE - Law enforcement capabilities in relation to child exploitation

To help ensure anonymity, dark web browsers isolate sites to prevent tracing, automatically clear browsing history, prevent surveillance of connections, clone or dupe users' appearances to avoid fingerprinting and relay and encrypt traffic three times as it runs across the network. Because access to specific secret sites is required, criminals that use the dark web to plan their activities can hide these activities and work hard to ensure their groups are not infiltrated by law enforcement. Hence, given the anonymity the dark web affords, it is unsurprising it has been exploited by a wide range of criminal actors for communication and the sale of illicit materials.

While there is legislation that supports law enforcement accessing encrypted communications, notably the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* and the *Surveillance Legislation Amendment (Intercept and Disrupt) Act 2021*, both pieces of legislation (rightfully) have high thresholds for the granting of warrants and often rely on the cooperation of private organisation in foreign jurisdictions for disclosures.

Cryptocurrency

Cryptocurrencies (also referred to as crypto) are an intangible, internet-native currency enabling almost instant borderless transfers, which can be utilised to quickly transfer the proceeds of crime across jurisdictions. This, as well as the relative anonymity provided by peer-to-peer cryptocurrency transactions, is attractive to cybercriminals, providing a layer of obfuscation for transactions without the challenges of cash transactions or cash transportation.

As noted by a Department of Home Affairs' Cyber Security Industry Advisory committee report into cryptocurrency in 2022, there has been an increase in organised crime exploring the use of cryptocurrencies to conduct or facilitate cybercrime and launder money. The report states: "Cryptocurrencies are being widely used for cybercrime exploits, including ransomware attacks, business email compromise, malicious cryptocurrency mining and the sale of malware. They are also used to buy and sell illicit goods and services on the dark web, including weapons, drugs and child sexual exploitation material. To face the challenges criminal use of cryptocurrencies present, traditional law enforcement methodologies require adaptation. Relationships with industry, training of investigators and appropriate regulation of cryptocurrencies and their use and exchange will be vital to meeting this challenge as the use of cryptocurrencies increases".[40]

While cryptocurrency regulation in Australia is evolving, crypto remains an attractive form of currency for criminals.[41] In Australia, law enforcement has met the challenge head on, with the establishment of a specialist AFP cryptocurrency unit in 2020, which targets money laundering as more criminals seek to bypass the financial system and funnel money offshore via crypto exchanges. So far, the unit has had significant success in seizing cryptocurrency in proceeds of crime actions.[42] Furthermore, in 2023, the AFP launched Operation Avarus, a multi-agency taskforce to target criminals laundering money, including via crypto.[43]

[40] Exploring Cryptocurrency (homeaffairs.gov.au)
[41] Crypto-assets: The case for strong regulation and enforcement | ASIC
[42] Australian Federal Police forms cryptocurrency unit to hit criminals (afr.com)
[43] New money laundering taskforce tackles lifeblood of organised crime | Australian Federal Police (afp.gov.au)

Keeping up with crypto remains a significant challenge requiring global collaboration. The AFP participates in the Five Eyes Law Enforcement Group's Money Laundering Community of Practice, which brings together senior law enforcement leaders and subject matter experts to share intelligence and cooperate on international operations.[44] The ICTRF also addresses crypto related challenges.

While cracking the crypto challenge is difficult, a 'follow the money' approach has been applied by law enforcement with some success. For example, when US fuel-distributor Colonial Pipeline was the target of a 2021 ransomware attack the company paid a ransom to recover access to its data. However, the Federal Bureau of Investigation (FBI) was ultimately able to recover about US$2.3 million of the ransom payment by obtaining a private key to unlock a crypto wallet.[45] The CSCRC submits there is merit in work being undertaken to investigate and identify how 'follow the money' approaches could be more effectively implemented by law enforcement domestically and internationally.

Emerging issues

As this submission repeatedly highlights, cybercrime is dynamic and continuously evolving. And, like governments and the private sector, cybercriminals are always seeking out new technologies that can enhance their operations. Furthermore, they can undertake such pursuits without the regulatory and ethical guardrails others must follow.

While there are many emerging technologies that impact the digital domain, the CSCRC submits that AI and the Internet of Things (IoT), when fully realised, have the potential to transform the way cybercriminals operate. They may also make it more difficult to detect, investigate and prosecute cybercrime.

These are issues the CSCRC has explored deeply in recent policy papers, which are noted below. Rather than look at these issues broadly, this submission highlights the issues raised in the papers, which could have significant implications for cybercrime law enforcement.

AI and cybercrime

Frontier AI technologies and their intersection with cybercrime has been an area of significant interest for the CSCRC. While there has been noteworthy commentary regarding this issue in relation to specific threat types like deepfakes, AI-enabled cyber attacks, tailored and sophisticated large-scale phishing exploits, and the spread of disinformation, little information has been paid to the exploitation of AI systems themselves.

In October 2023, the CSCRC released *Poison the well: AI, data integrity and emerging cyber threats*, which highlights emerging cyber threats that could arise through the increased application of generative AI systems, namely large language models (LLMs).[46] These threats include data poisoning attacks on AI data training sets and cyber threats associated with human labelling of AI data sets.

[44] New money laundering taskforce tackles lifeblood of organised crime | Australian Federal Police (afp.gov.au)
[45] Shifting crypto landscape threatens crime investigations and sanctions | Brookings
[46] Poison the well - AI, data integrity and emerging cyber threats.pdf (cybersecuritycrc.org.au)

In the world of AI, data accuracy and integrity are everything. If data is incorrect or is biased it means an AI system will not be fair or accurate, ultimately making it untrustworthy. Therefore, any threat to AI data inputs presents a threat to the integrity of an AI system itself and, more worryingly, could have serious societal impacts. Hence, cyber attacks aimed at manipulating AI data sets must be considered as a serious emerging cyber threat vector of which law enforcement, needs to be increasingly aware.[47]

Data poisoning attacks occur when an AI system is being trained. Such attacks involve the input of malicious, biased or incorrect data into an AI data training set, resulting in the model learning false patterns and making incorrect connections. Hence, when a poisoned model is deployed, it will produce incorrect outputs that could enable an attacker to bias decision-making towards a particular outcome, which could lead to real-life harms.[48]

The paper also raises the spectre of poor workers and corrupt officials in developing nations, where much LLM data labelling is outsourced, that may be particularly vulnerable to coercion by malicious parties, who could employ financial incentives to use such a workforce to manipulate the labelling of LLM training data. Such attacks, known as label poisoning and input attacks, occur when an adversary injects mislabelled or malicious data into an AI training set to influence its behaviour and alter its outputs. In effect, this could see offensive materials or text sequences, like that related to child abuse material or rape, intentionally incorrectly labelled as something harmless, like a tree, cat or bag. If this was to occur at scale across a range of different damaging scenarios – and research indicates only 0.01% of training data needs to be poisoned to be effective – the impacts on LLMs could be serious and the implications for society damaging. Most importantly, such an attack would have a deleterious impact on perceptions of GAI at a social and cultural level, impacting the positive economic and societal effects these technologies can affect.[49]

While there is no evidence that such attacks have yet occurred, other forms of cyber-based poisoning, like malware, are well known threat vectors. Therefore, with potential attacks on AI training data sets seemingly inevitable, it is an emerging issue that policy makers must consider.[50]

IoT and cybercrime

There are currently more than 15 billion operational internet of things (IoT) devices in the world – almost two for every person. And this number is expected to explode, with IoT proliferation set to hit 30 billion devices by 2030.[51] These devices are central to our everyday lives – we hold them, we wear them, we watch them and, increasingly, our critical infrastructure relies on them to operate effectively.

Despite the increasing ubiquitousness of IoT and their vulnerability to exploitation, there is no regulation that directly governs their cyber security, noting this is an issue the government aims to

[47] Poison the well - AI, data integrity and emerging cyber threats.pdf (cybersecuritycrc.org.au)
[48] Ibid
[49] Ibid
[50] Ibid
[51] IoT connected devices worldwide 2019-2030 | Statista

tackle through the *2023-30 Australian Cyber Security Strategy*.[52] Furthermore, due to their sheer volume, little attention has been paid to IoT as a vector for cybercrime.

While the CSCRC has not analysed IoT cybercrime broadly, we have examined the cyber security and potential for cybercrimes to be committed via photovoltaic inverters (solar inverters). Not only are solar inverters IoT devices that collect and distribute valuable data, but they also play an increasingly vital role in Australia's energy security.

In August 2023, the CSCRC released *Power out? Solar inverters and the silent cyber threat*, a report that addresses cyber threats associated with solar inverters and the threat of critical infrastructure disruption.[53]

Traditionally, the cyber risk associated with solar inverters was low because they were not connected to the internet. However, as the popularity of smart home energy systems has boomed, this has changed, with most solar inverters now web connected for monitoring and control purposes. In turn, this has increased the cyber-attack surface of solar systems and, as internet-connected devices, solar inverters are vulnerable to a range of cyber intrusions including hacking, malware attacks, manipulation and disruption. Therefore, as the number of homes with solar systems continues to increase, the risk associated with solar inverters continues to grow.

Since 2020, the Cyber Security Cooperative Research Centre (CSCRC) has funded University of New South Wales (UNSW) research exploring cyber security threats to DER. As part of the project, researchers have examined cyber threats to solar inverters, running two simulations to illustrate how different attack vectors impact their function.

In the first simulation, command data between a solar inverter and a home energy management system was intercepted, then replayed to the solar inverter using a replay attack script. As a result, the solar inverter was able to be turned off and energy supply cut.

The second simulation involved an attack on a web service provider to which a solar inverter was connected. The web interface was disabled using a command injection technique, meaning owner access to the solar inverter was blocked, preventing remote control and monitoring.

While such attacks on one home solar system would not impact the grid more broadly, scaled, targeted simultaneous attacks could be catastrophic. CSCRC Director of Research Professor Helge Janicke said that a widespread attack aimed at solar inverters had the potential to bring down an entire power grid, which could result in a 'black start' event. It could take a week to recover from a black start because power plants would be incapable of turning back on, without reliance on an auxiliary power source.

[52] 2023-2030 Australian Cyber Security Strategy (homeaffairs.gov.au)
[53] Power out? Solar inverters and the silent cyber threat (cybersecuritycrc.org.au)