Tor's underworld, 'onion services' and child sex abuse material: Submission to the Australian Parliamentary Joint Committee on Law Enforcement inquiry into 'Law enforcement capabilities in relation to child exploitation'

September 21, 2021

Roderic Broadhurst* and Matthew Ball**
Australian National University Cybercrime Observatory[1]

*Emeritus Professor, Department of Regulation and Global Governance
**Research Officer, Cybercrime Observatory, Department of Regulation and Global Governance

[1] This submission addresses the prevalence of CSAM on the Tor anonymous internet service and reports preliminary data from the ANU's Cybercrime Observatory's 'Tor Universe' research project led by Professor Ross Maller and Emeritus Professor Roderic Broadhurst. Observatory researchers Justin (Haotian) Weng and Jessie (Chuxuan) Jiang contributed to this submission.

Summary

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020[2], which passed both houses of parliament on August 25, 2021, will assist law enforcement agencies (LEAs) in investigating serious crime including online child sex abuse materials (CSAM). Despite relevant tools such as data disruption, network activity and account takeover warrants, LEAs will nevertheless encounter challenges in the darkweb – notably Tor (formerly known as The Onion Router), the largest of the anonymous platforms.

Anonymous Internet services, such as Tor, are designed to evade surveillance and its highly decentralised structure is resilient despite the periodic success of cross-jurisdictional policing operations in disrupting, arresting, and closing both illicit contraband markets and CSAM sites on Tor (Broadhurst, et al., 2021). The deterrent effect of LEA operations tends to be short lived, but can influence the perceptions of risk and deter potential offenders. LEA operations also can stimulate self-regulation (e.g., banning and/or censoring particular products or interests) among some relevant Tor hidden or 'onion' service providers. Anonymity also provides opportunities to reach out to existing support 'communities' among these online secretive sub-cultures and seek support in crafting relevant online health, education and treatment referral services.

Most illicit markets active on the Tor network ban CSAM and other violent abuse materials as well as weapons and poisons, COVID-19 vaccines, and other dangerous products. However, specialist onion services cater for these banned products as well as for paedophilia, paraphilia and other extreme interests that could constitute abhorrent violent conduct as defined by the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019[3].

The Tor environment offers online actors' greater anonymity and they behave differently to how they behave in standard online environments (i.e., Reddit, Facebook). This is demonstrated by the presence of CSAM and other abhorrent material on Tor as we recently reported. CSAM is also common on clearnet and through peer-to-peer (P2P) services but the material on Tor is more egregious, often involving younger victims and violent abuse, than is typically encountered on the surface web (ECPAT, 2018).

[2] Amends the Commonwealth Criminal Code 1995, *Surveillance Devices Act 2004,* and *Telecommunications (Interception and Access) Act.*

[3] Enacted in the wake of the 2019 Christchurch terrorist incident the act defines abhorrent violent material as the most egregious, violent audio, visual or audio-visual material produced by a perpetrator or their accomplice. The definition includes video, still images (and series of images) and audio recordings but excludes material recording animated, reenacted, or fictionalised conduct. Such material must stream or record conduct where a person engages in a terrorist act (involving serious physical harm or death of another person), murders or attempts to murder, tortures, rapes or kidnaps another person (where the kidnapping involves violence or the threat of violence).

The well known limits of the deterrence approach have long pushed policymakers to foster broader public health and harm reduction strategies to reduce violence and abuse in all settings, especially domestic violence (and child abuse) and its dire long term impacts on children. A similar broad approach (the carrot as well as the stick) also needs to be implemented to aid the suppression of online CSAM and other illicit abuse materials. Partnerships between the technology industry and LEA are vital but have limits. Survivor and victim support groups also play a key role and have a potent voice in confronting offenders. Getting the message to offenders and efforts to reach and treat non-contact online CSAM 'consumers', however, are fraught and under-developed.

Spurred by deterrence, shame, or other motivations the limited research about online CSAM offenders indicates that a significant proportion can be helped to desist: i.e., treatable. To capitalise on opportunities for treatment, self-help, helplines and education engagement by civil society actors such as specialist legal and health services (sex abuse desistance programs) with Tor 'community' forums (and other anonymous platforms) is required. The anonymity of Tor can be effectively used to reach these secretive communities and through their nascent self-help efforts explore pragmatic opportunities for harm reduction. Initiatives to improve efforts to suppress CSAM and respond to the impact of the pandemic on child protection are needed (UNICEF, 2020).

Since April 2019 Swedish researchers have trailled "prevent It" an anonymous online cognitive behavioral therapy (CBT) program provided via a Tor service aimed directly at active online child sex offenders (see Figure 3). The eight week online program is built into a blinded randomised clinical trial to gauge whether it is effective in decreasing consumption of CSAM (Parks, et al., 2020). An evaluation is pending. It is this overlooked element of the prevention puzzle, directly engaging with offenders in treatment and desistance behaviour, that this submission argues warrants further attention, support and research.

This submission considers the capability of Australia's law enforcement agencies to tackle the growing scourge of child exploitation. In particular, concern about the existence of dedicated CSAM onion services hosted on the Tor network were raised (Terms of Reference [a]). This also required an understanding of the tools used by offenders to access CSAM and the ability of law enforcement to detect CSAM and identify offenders (Terms of Reference [d]). We suggest specific support be provided to develop and evaluate online treatment programs for CSAM offenders using the anonymous format provided by Tor . Finally, we propose a study examining the links between offline and online/contact and non-contact offenders in the context of anonymity (Terms of Reference [f]).

Introduction

In August this year, Apple made news by announcing, and then delaying, its plans to check US iPhone users' photo libraries for known CSAM if stored in the online iCloud service and other improvements to its child safety features. Policy groups promptly raised issues about this scanning service, citing violations of protected speech, infringements upon the privacy and security of Apple users, and potentially even damage to the children the service intends to protect[4]. Privacy concerns notwithstanding, this is another attempt by big technology companies to combat the online pervasion of CSAM. The Apple 'case' illustrates the limits of industry and LEA cooperation especially where systematic scanning of servers is involved, even where US law requires reporting CSAM to the non-profit US National Center for Missing and Exploited Children (NCMEC).

Many other platforms (e.g., Facebook, Google, Dropbox, Twitter, Microsoft and Snapchat) also scan for CSAM against known databases, such as the image repository held by the NCMEC[5] and others widely used by LEAs across the world[6]. These databases consist mainly of image file hash values, but, more recently, are including video hash file values[7].

In July 2021 the European parliament in accord with the Council of Europe's Lanzarote Convention (2007), which promotes measures to prevent online child sex abuse, implemented temporary measures to enable technology companies to legally scan online messages for CSAM pending legislation that could make it mandatory for technology companies to do so. The growing appetite for further legislation and regulation of the role of big technology in the suppression of CSAM and other abhorrent material will be controversial and cannot be reduced to a trade-off between privacy, free speech or child protection. Child sex abuse is not a free speech or privacy issue but a harmful crime of domination sheltered and facilitated by anonymity platforms and encrypted social media services.

One survivor explained: 'The abuse stops and at some point, also the fear of abuse; the fear of the material never ends.' (Canadian Centre for Child Protection, 2017, p. 149). Survivors of CEM often suffer post-traumatic stress disorder (Hannan, Orcutt, Miron & Thompson, 2015). Images

[4] The potential risk of the (image) content-matching process being re-purposed to detect other objectionable content is a prime concern along with the probable presence of false positives, and potential malicious gaming of the system (e.g., planting of CSAM); see Jonathan Mayer, Anunay Kulshrestha (August 19, 2021) 'Opinion: We built a system like Apple's to flag child sexual abuse material — and concluded the tech was dangerous', Washington Post.

[5] In 2020 the NCMEC received 21.7 million CSAM reports, up from 16.9 million in 2019. Apple made few reports (265) compared to Facebook's 20.3 million reports, Google made 546,704; Dropbox 20,928; Twitter 65,062, Microsoft 96,776; and Snapchat 144,095 (cited in Burgess, 2021).

[6] For example: the UK internet Watch Foundation, Interpol Child Abuse Image Database (ICAID), International Child Sexual Exploitation Database (ICSE-DB), and the Australian National Victim Image Library (ANVIL)

[7] A hash value is a numeric value of a fixed length that uniquely identifies data - a digital fingerprint for a file.

can be replicated and shared again. Victims experience anxiety using the Internet because their image may reappear and they will be traumatized again. This constant re-victimization process and stress impact day-to-day functioning, degrades quality of life, increases potential physiological and mental harm, and negatively affects life course (Canadian Centre for Child Protection, 2017).

Despite the efforts that big technology companies and governments have devoted to detection (e.g., Microsoft's PhotoDNA; Google; Thorn), CSAM is still rampant online[8] and amplified by the COVID-19 pandemic[9]. It is in the anonymous Internet - the 'darknet' or 'darkweb' - where communities can share this material with little fear of prosecution.

There are few platforms offering anonymous Internet, with i2p, FreeNet, and Tor being the best known. The most widely used of these overlay networks, Tor, presents a conundrum. Online privacy advocates have championed its benefits and uses, claiming that the Tor network protects free speech, freedom of thought, and civil rights. However, Tor has a dark side too. Academic studies and the Tor project themselves have long acknowledged the potential for misuse of the service (for example, see "Doesn't Tor enable criminals to do bad things?"; Minárik and Osula, 2015; Owen and Savage, 2016) and when combined with technologies such as untraceable cryptocurrencies, the possibility for criminals to hide their activities poses a real threat.

Tor (Formerly The Onion Router)

Tor is an overlay network that exists "on top" of the Internet and merges two technologies. The first is the onion service software. These are the websites, or "onion services", hosted on the Tor network. These sites require an onion address and their servers' physical locations are hidden from users. The second is Tor's privacy-maximising browser. It enables users to browse the internet anonymously by hiding their identity and location. While the Tor browser is needed to access onion services, it can also be used to browse the "surface" Internet (the world wide web [WWW]). The Tor network is based on a mix-routing principle. Communication over the Tor network is analogous to the layers of an onion: starting from one node (an entry/guard relay) encrypted traffic passes through multiple nodes, at each node the traffic is further encrypted and repacked, effectively making the traffic invisible until it finally reaches an exit node at another Tor gateway.

Accessing the Tor network is trivial; simply download the requisite web-browser. While search engine options are limited (there's no Google), discovering onion services is simple. The BBC, New York Times, ProPublica, Facebook, the CIA and Pornhub all have a verified presence on Tor

[8] In 2018 alone, Europol reported over 46 million images and videos of CSAM online, double what was reported in 2017. The Australian Centre to Counter Child Exploitation (ACCCE) received over 21,000 reports of online child sex exploitation in 2020 and examined over 250,000 CSAM images.
[9] A world-wide trend also evident in Australia: see Salter, M., & W.K. Wong, 2021 "The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing".

network, but it is through the 'service dictionaries' of the network, such as "The Hidden Wiki", that users are able to discover other - often illicit - services. Among these services are those that provide unmoderated pornographic content, including CSAM.

Live-stream CSAM has been documented using end-to-end encryption (E2E) services (see: ECPAT, 2017, Brown, Napier, and Smith, 2020) and CSAM can still be found, notably in peer-to-peer (P2P) networks on the clearnet. P2P networks are popular because they are free and publicly accessible and can distribute CSAM without using Internet service providers. P2P networks can also be anonymous and users can avoid contact altogether because the shared folder acts as a blind link (Lee, *et al.,* 2020). However, onion services that *live-stream* sexual violence, torture and murder and other abuse on Tor has not been detected; given Tor's limitations[10], and other options available to producers of CSAM live-stream activity, onion services could best be used to advertise such services and/or archive copies of such activity. Nevertheless, horrific stories about 'Red Rooms' on the darkweb, are rumours spread for their shock value and spawn scams intended to monetize the prurient interest in them.

Tor's Underworld

It's difficult to identify what exactly is available on Tor's onion services. Many services and content available are camouflage for scams or simply inaccessible. The number of onion services active on the Tor network is unknown, although the Tor project estimates about 170,000 active onion addresses - this is a fraction of the number of websites accessible over the surface Internet (the world wide web). The architecture of the network allows[11] partial monitoring of the network traffic and a summary of which onion services are visited. Among these visited onion services, CSAM is common.

Most users access the Tor network to retain their privacy online, rather than use the anonymous onion services. Of the estimated 2.6 million users that use the Tor network daily,[12] 21,718 (including 418 via a bridge) requests originated from an Australian Internet address (this does not equate to individuals, as requests for access and a user may make multiple requests). Owen & Savage (2016) reported that only 2% (52,000) of the users access onion services. They also

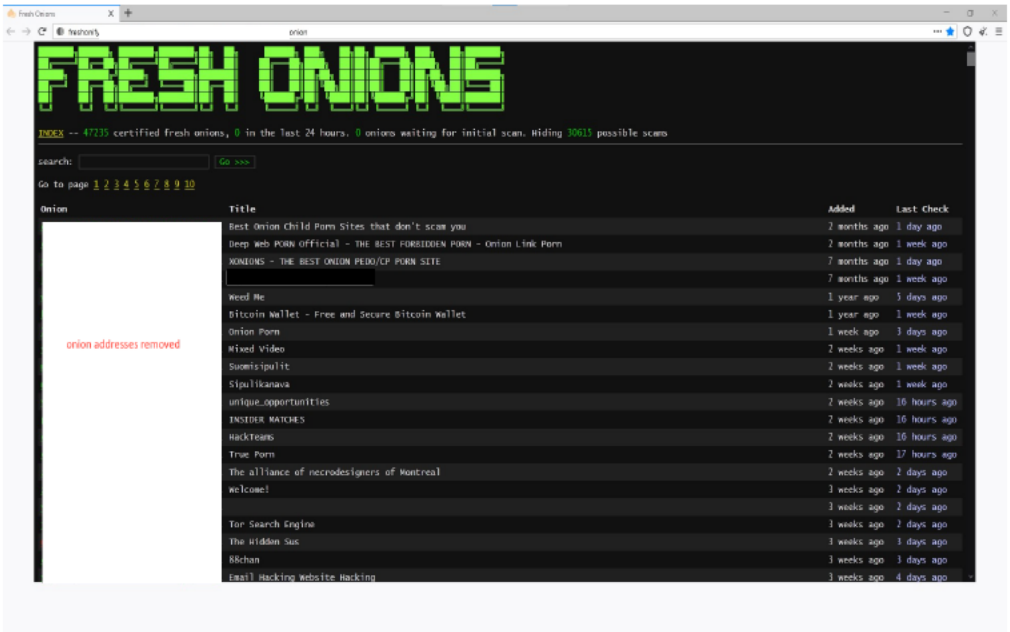
[10] Tor's network performance data reports onion service performance for static files averaging between 2-5 seconds per 1MB and 10-30 seconds per 5MB suggests that a live stream service would require significant adjustments to manage upload.
[11] According to the Tor project this changes with the depreciation of v2 address formats and the crossover to v3 come October 15th, 2021.
[12] On 6 September 2021 there were 2,590,051 clients via relays and 44,449 via bridge nodes. Estimates vary over time, for example on September 14th, 2021 Tor estimated there were 2,362,291 clients including (50,126 via bridges) bridges of whom 22,676 were Australian users - 510 connected via a bridge. For comparison users accessing via a *relay*, included 191,343 client requests from German users; 62,728 users from Great Britain; 53,496 from the Netherlands; 20,684 from South Korea; 335,026 Russian users; 506,719 from USA; 39,873 from Canada; 31,494, Thai users; 15,867 from Iran; and, 49,338 users from the Ukraine.

found that approximately 80% of this traffic to onion services (42,000) was directed towards services which offered unmoderated porn, including CSAM[13]. Another study by Ternium Labs in 2016 found that 53.4% of all active onion domains contained legal content, suggesting that 46.6% of the services were of grey or illegal content. Spitters, et al., (2014, p. 223) estimated that 17% of the platforms in their collection of 5,725 onion services (about 1,450 concurrent/active at any time in 2013) consisted of "adult content" and about half of this pornography was classified as CSAM.[14]

Tor Onion Services

Attempts to map and describe the Tor 'universe' are challenging as it is dynamic and ephemeral - much is obscured and unknown. It is possible only to describe those onion services, usually a web page, that are openly available to those browsing Tor. Some services use multiple onion addresses/URLs and duplicates as well as scam sites are common. Many other Tor services are present but require a login or invitation and remain invisible to researchers. There are two notable ways of identifying active onion services.

Figure 1: Example of a Tor index of onion addresses (September, 20, 2021)



Note: onion addresses deleted

The first method involves running a Tor guard node (relay) and recording both client numbers and destination onion service addresses as traffic which passes through the relay. As of

[13] Even though this figure appears high, this is only 1.6% of all users on the Tor network.
[14] Spitters, et al., (2014, p. 223) noting the difficulties of topic classification also "...found hidden services with more noble intentions, discussing political oppression, freedom, and anonymity. However, because topics cannot easily be mapped to intentions (think of disclosing confidential documents, anarchic communities, doxing), it is very hard to unambiguously divide our Tor data into a 'good' and a 'bad' part."

September 6th 2021, there are 7,045 public relays or guard nodes (IP address [i.e., identity] known) and 1,366 private relays or Bridge nodes (IP address unknown) - a total of 8,411 relays - in use. A client passes through at least three relays before reaching the destination service, but the number of passed relays can be as high as seven[15].

A number of directories provide lists of onion addresses (URLs) that have been requested rather than outdated wiki or user-submitted links (see Fresh Onions below). For example 'live' onion miner GIMPYD[16] observes onion links passing through its guard node relay(s) and currently lists 7,360 onion services (since July 2nd 2019) but also records the number of users (client requests). Most traffic was to Hydra, a Russian darknet market, but other illicit services, including unmoderated pornography, were active and visited.

This method (observational sample) is the most effective over time and produces more than just web-based onion services. However, this method relies on a particular way that v2 addresses are stored/recorded. With the Tor project retiring v2 addresses on the 15th of October 2021 it will no longer be possible to estimate the number of onion addresses[17].

The second method is limited only to web-based onion services - but does identify the services which are most easily identifiable by users (Owenson, Cortes, & Lewman, 2018). This method involves recording onion addresses from a list of known service dictionaries or indices, such as "The Hidden Wiki". Onion services indexed include many illicit services and these URLs seed and bias the crawler used to capture data from onion services and consequently .

We describe the 'public facing' (i.e., web-based) services identified in our ongoing research on the scope of onion services on Tor. In the table below we broadly classify 25,913 onion addresses identified by our crawler in August 2021. This compares with the 47,230 onion addresses (not accounting for duplicate services) indexed on the popular Tor (user-submitted and compiled) listing service Fresh Onions, although a third or more of these links are estimated to be inactive (see Figure 1). Just over half of the addresses we identified were distinct services[18] (51.5%; n=13,342) and over 30% of all addresses were active (31.6%; n=8,184).

---

[15] It follows that the number of clients passing through a specific relay each day is at least 757 and at most 2,018 (on average 1,387).

[16] GIMPYD headlines itself: "Welcome to the gutter of the Internet".

[17] From a technical perspective, there are 1,208,925,819,614,629,174,706,176 possible v2 onion addresses and 7,237,005,577,332,262,213,973,186,563,042,994,240,829,374,041,602,535,252,466,099,000,494,570,602,496 possible v3 onion addresses. Only a very small fraction of these addresses are used. The Tor project reports that there are 136,229 active v2 onion addresses as of 7th of September 2021, down from a high of 232,398 active v2 onion addresses recorded on the 11th of May 2020. Statistics for v3 addresses are unknown but the decline in v2 onion addresses since May 2020 may be explained as services move to (new) v3 onion addresses before the Tor project officially deprecates the v2 address space on October 15, 2021.

[18] Duplicates of the same service are removed: i.e., when website descriptions match more than one address (many onion services operate several addresses or mirrors).

Table 1: Tor onion services – preliminary classification

Service category	**count of 'distinct'* services N**	**count of services %**	**active services N**	**active services %**	**address counts N**	**address counts %**
counterfeit	4215	31.59	2577	31.49	11000	42.45
cryptocurrency	1914	14.34	1119	13.67	2702	10.43
markets	857	6.42	463	5.67	1487	5.74
no access	942	7.03	502	6.13	2532	9.77
other	268	2.01	144	1.76	359	1.38
porn	2353	17.63	1791	21.88	2915	11.25
security	271	2.03	140	1.71	344	1.33
services	2184	16.36	1247	15.24	3851	14.86
non-English	338	2.53	201	2.456	723	2.79
Total	**13342**	**100%**	**8184**	**100%**	**25913**	**100%**

Source: ANU Cybercrime Observatory computer file (16.8.2021). *Notes:* * distinct services after accounting for duplicates. Categories comprise: Cryptocurrency services - Bitcoin and other exchanges, mixers, mining, wallet services, money laundering; Markets - general and specialist that sell illicit drugs, weapons, malware and other contraband; Counterfeit products - currency, credit card markets, stolen data base, credentials, passports and other documents; Services - hacking, doxing, DDOS, botnets and other specialist malware such as ransomware tools, indexes, news services; Security - services for operational security of a darknet market, bullet-proof hosting; Porn - unmoderated pornography including CSAM, and other illicit images of sexual abuse.; No access - require passwords/ tokens/invitations; Non-English sites; Other - services not classified elsewhere.

The available data does not permit estimates of the number of users who visit onion services: while a service may be active it nevertheless may attract few, if any, visitors. 'Porn' which comprises unmoderated content and includes CSAM, other abuse and illicit images accounted for 11.25% of all addresses (n=2,915) and 17.6% (n=2,353) of the distinct services but 21.9%

(n=1,791) of the *active* onion services. Only onion services offering counterfeit products (31.5%; n=2,577) exceeded unmoderated 'porn' among all active addresses.

CSAM Onion Services

While scams make up a significant proportion of onion services, hobbyists, tinkerers, cryptocurrency services, dealers in drugs, malware, weapons, stolen credentials, counterfeit products, and CSAM also populate this 'dark corner' of the Internet. Only about 7.5% of the CSAM on the Tor network is estimated to be sold for a profit. The majority of those involved are not in it for monetary purposes; most CSAM is simply 'swapped'[19] but a profit driven model has emerged with some services charging fees for content[20].

Figure 2: W2V Seizure, March 5 2018

The Welcome to Video (W2V) onion service is an example of a website that gives users a forum to trade in CSAM images. Operating between July 2015 and March 2018 by a 23 year old South-Korean national, W2V offered over 250,000 videos and images (eight terabytes of media involving CSAM) - 45% of which featured "fresh" or previously unidentified content and victims. Known downloads amounted to 360,000 requests, yet W2V claimed to have facilitated one million downloads from its 1.28 million members (4,000 of which were paying customers) from 38 countries. Customers paid using cryptocurrencies, in particular Bitcoin. When the service was

[19] A common condition of entry to CSAM sites is for the user to upload such images to the site binding all players to a conspiracy to possess and distribute illicit content.

[20] Europol's 2021 organised crime assessment observed "...a continuous increase in activities related to online child sex abuse over recent years" (Europol, 2021, p. 41). Europol's 2020 Internet Organised Threat Assessment stressed increased risks arising from COVID and noted CSAM live streaming was becoming more mainstream. "Although offenders are still primarily driven by a desire to obtain more CSAM... The emergence of a profit-driven model in this crime area is a worrisome development" (Europol, 2020, p. 40).

taken down by a cross-jurisdictional LEA operation in March 2018 (see Figure 2), it was estimated to have made USD370,000.

Several high-profile onion services hosting CSAM have been shut down following extensive cross-jurisdictional law enforcement operations, including The Love Zone[21] in 2014, PlayPen[22] in 2015, and Child's Play[23] and Elysium[24] in 2017. A recent investigation led by German police, and involving others including Australian Federal Police, Europol and the FBI, resulted in the shutdown of the Boystown[25] in May 2021 which had been in operation since June 2019.

LEAs are not the only actors attempting to disrupt CSAM on the darkweb. In 2017 the online activist group Anonymous hacked Freedom Hosting II, removing a reported 10,000 onion services, including CSAM services. Accounting for an estimated 15-20% of CSAM hosted on the darkweb at the time (Burgess, 2017).

Hosted as an onion service since 2010, Lolita City is one of the largest CSAM forums on the Internet - not just Tor. It has evaded law enforcement (and activist) takedown attempts over the past decade, boasting 508,721 registered users (as of August 2021) and 1.3 million pictures and videos since June 2013, with 100gb of pictures since 2011. While Lolita City is an outlier in its size and reach, these CSAM trading forums are common. There are at least a dozen such forums active at any time. While some of these forums are open, enabling observation without registration, the majority are closed and require registration.

Given the volatility and ephemeral nature of Tor onion services, a focus on onion directories or lists and forums offer opportunities for harm reduction. We know little about Tor CSAM interest forums and their interdependency with services may account for the volatility and shifting trends. Monitoring forums may reveal actionable interventions and engagement could allow the feasibility of treatment and self-regulatory conduct to be explored. Before addressing the promise and challenges of online harm reduction programs for CSAM offenders/consumers we briefly review countermeasures available to LEAs.

Law Enforcement and Countermeasures

Law enforcement and government agencies face difficulties surveilling and policing the darknet. This difficulty as emphasised comes from the privacy and anonymity afforded by layered Internet

[21] An estimated 45,000 users accessed this onion service.
[22] Operation Pacifier undertaken by Europol (European Cybercrime Centre) and the FBI. PlayPen operated between August 2014 to February 2015, featured 214,000 registered accounts, 117,000 postings and, as of May 2017, Operation Pacifier had identified or rescued 351 sexually abused children and 808 arrests.
[23] At its peak, Child's Play was estimated to have over one million users.
[24] There were 111,000 registered user accounts. As of July 2017, 14 suspects and 29 victims have been identified.
[25] Boystown was estimated to have 400,000 registered users and operated two chat services. The operation resulted in the arrest of three German nationals (one based in Paraguay).

technology, such as Tor. As Liggett, et al., (2020, p. 108) stress: "In order to successfully identify anonymous darkweb users engaging with CSAM, federal law enforcement must rely on third-party reporting, international cooperation, and complex technical skills, making the illicit online sex market difficult to disrupt". In short most darknet investigations require resource intensive cross-jurisdictional collaborative efforts.

Significant challenges face LEAs in the prosecution of the producers and distributors of online CSAM because criminal activity typically falls across multiple jurisdictions (offenders may be in one jurisdiction and victims in another but the evidence in a third), making detection and prosecution difficult. Re-tooled for the digital environment, undercover and controlled operations and new online investigative techniques (i.e., targeted 'hacks' and malware) are essential. These operations are facilitated by mutual legal assistance (MLA) treaties. Two key treaties the 2001 Council of Europe's Convention on Cybercrime[26] and the United Nations Convention on Transnational Organised Crime[27] (UNTOCC), address child sex abuse material and the trafficking of women and children.

Another barrier is the absence of a universal definition of 'child' or CSAM, and the legal age of consent varies across the globe (Wortley & Smallbone 2012). These challenges can be resolved by comity as exemplified by the Council of Europe's Lanzarote Convention, which harmonizes the legal definitions of sexual offences against children as well as measures to protect victims and prosecute offenders. Continued efforts to harmonise the relevant laws across the world are needed even in Australia where federation has created a patchwork of differences in the age of consent and the definition of CSAM offences.

The International Centre for Missing & Exploited Children (ICMEC) reported that 118 of the 196 countries in its survey of laws aimed at criminalising CSAM had four of five necessary measures in place[28]. Sixteen countries had no CSAM specific laws and only 21 nations had all five legal requirements available with many countries failing to criminalise possession or mandate reporting of CSAM - the latter essential if CSAM image databases are to be shared, grown and used to increase detection (cited in Lee, et al., 2021).

[26] Sixty-seven countries, Australia, Japan, USA among them have adopted these measures since 2001. A further 11 countries are in the process of ratification or have been invited to accede to the convention, however, Russia, China amongst others have not, although parties to the UNTOC thus widening the scope of police to police assistance in these matters.

[27] In particular the additional 'Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children' extend the remit of the UNTOCC (Article 3), to include "…the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs".

[28] (1) National Laws with specific regard to CSAM, (2) CSAM definition, (3) criminalization of technology-facilitated CSAM offenses (4) criminalise possession, regardless of the intent to distribute, (5) Internet Service Providers' (ISPs) required to report suspected CSAM to law enforcement or other mandated agency (cf ICMEC).

Harmonised national CSAM laws, MLA treaties, along with international agencies such as Interpol, United Nations Office of Drugs and Crime (UNODC), national, regional and other international law enforcement alliances combined with industry partnerships and civil society actors such as the WeProtect Global Alliance, INHOPE, ECPAT and many others provide a growing, if yet seamless web of cooperation that can help suppress CSAM.

Repurposed and Novel Investigative Techniques

Unpacking LEA online capability helps situate present challenges and opportunities. As with traditional (offline) investigations, there are two operational contexts: *proactive* investigations that focus on automated, covert and manual intelligence gathering, indexing for future use (potential) threats and usually targeting known suspects or organisations (e.g., web crawlers, covert operations); and *reactive* investigations that respond to criminal incidents and reports (attribution, de-anonymization). However, LEAs are essentially driven by complaints (by victims and others), and event/incident discovery, which in turn impacts caseload triage and resource allocation. Complaints about CSAM frequently involve high priority cases of missing and abused children (especially contact offenders who produce CSAM) and high volume crimes (possession and online consumption of CSAM) that require specialist services and responses.

In the context of the Tor network, LEA operations have relied on two methods:

1. Exploitation of user mistakes (the most common vector): people can become complacent with their operational security (opsec) practices.
2. Exploitation of Tor's technical limitations and security issues: the design of Tor involves trade-offs between security and usability. LEAs could target three different entities of the network: a client of the Tor network; a Tor onion (hidden) service; and the Tor network itself (Cambiaso, et al., 2019, p. 3).

In the past, what has worked, although to varying degrees of success include: circuit reconstruction; timing pattern correlations; cookie leakage; and as noted - user error. Techniques that focus on the user/client such as linking darknet aliases to surface Internet aliases (Arabnezhad, et al., 2020) have been effectively employed. As law enforcement techniques become more known, and opsec practices tighten, this technique will only catch the "low-hanging fruit".

US government agencies developed a series of malware, known as the Network Investigative Technique (NIT), applied with effect in the shutdown of PlayPen and other Tor services. It is memory resident malware which exploits a vulnerability in the Tor web browser (in particular, it exploited a vulnerability in the Firefox web browser, which the Tor browser is based on). This exploit resulted in private information ("computer and internet protocol [IP] address verifier" [CIPAV]) from the users' computer being sent back to a law enforcement server outside of the

Tor network[29]. NIT 'hacks' nevertheless often rely on user error to seed/execute malware. The relevant browser bug fixes and other opsec features have subsequently been developed by forensically aware opsec providers to remodel and harden Tor web markets, forums and services.

A survey undertaken by Karunanayake, et al., (2021) drew upon 52 known attacks against Tor and reviewed the de-anonymization methods used. It noted the increasing difficulty of launching attacks on the network relays (by compromised entry/exit nodes) as the number of relays have rapidly increased. The use of trusted 'Guard' nodes as entry nodes offset the risk of new circuits being controlled by an adversary such as an LEA covert operation. A range of technologies, from ultrasound and watermark capture, that exploit Tor's traffic congestion controls have been considered in attempts to de-anonymise Tor. While machine learning approaches, webpage/website fingerprinting and a focus on onion services are potentially useful (Karunanayake, et al., 2021) these may be actionable, only when user error occurs.

The detection of CSAM via Internet report/helplines and CSAM filtering software currently rely on image hash databases, keywords, web-crawler, detection based on filenames and metadata, and visual inspection. The performance of CSAM detection tools also differ depending on whether a proactive crawler-based search tool (i.e., IWF and Arachnid) or a filtering (detection) service tool (Microsoft's PhotoDNA and Google's AI-based implementation) are used (Lee, et al., 2021). CSAM research, especially into detection methods, has also been impeded by the necessary restrictions around the possession of such data. This means limited testing of potential detection methodologies (in particular computer vision tools) against real data and images databases held by LEAs. A good deal more needs to be done to harness machine learning, image descriptors and multi-method (triangulation) in the identification of CSAM as well as reducing the impact of visual inspection on law officers.

The 'LEA vs techno-criminals' digital arms race continues to evolve and the most potent tools, such as 0 day exploits, or obfuscated surveillance tools (e.g., Pegasus like applications) if available, are likely to be sparingly used. These important limitations necessitate the need to explore other means of reducing the prevalence of CSAM: Perhaps most promising is the development of online tools and treatment programs that engage online CSAM consumers.

Lee, et al., (2020, p. 10) in a survey of online CSAM detection methods observe that it is "...crucial to understand the dynamics of perpetrators and their online communities. Key-words for web-crawling, for example, can change very quickly and can be ineffective if not adjusted". Detection methods of CSAM also need to consider the possibility of applicability across a variety of mobile devices and different platforms used for online interaction.

[29] In abstract terms, the NIT malware was composed of three components: 1. Generator: ran on the onion service, created a unique ID for each deployment, transmitted the ID, exploit, and payload; 2. Exploit: took advantage of the vulnerability in the Tor browser (Firefox); 3. Payload: sent the identifying information back to the FBI.

Secretive 'Communities'

The presence of CSAM onion services is well documented, with the hebephile, pedophile, and ephebophile[30] communities among early adopters of discussion forums, where members can share opsec practices and distribute media. The WeProtect Global Threat Assessment 2019 report estimated there were over 2.88 million users on ten forums operating via onion services. At the same time, onion service forums are being used for support among these paraphilia communities. As a widely condemned subculture these individuals wish to maintain their anonymity, and privacy when reaching out to talk to others with similar interests and concerns. Research about CSAM offenders and networks suggest that online 'consumers' may be a feasible focus for appropriately designed online programs. These 'safe havens' may offer opportunities for education, treatment and harm reduction.

Richards (2011) reviewed studies of CSAM offenders profile and found that it was not homogeneous and differences between contact and non-contact, offline and online, as well as cross-over online and contact offenders were evident. Eggins, et al., (2021, p. 12) systematic review of LEA responses to CSAM also note the characteristics, situation (online/offline) and causes differ among contact, non-contact mixed and CSAM only offenders are different but overlap. CSAM online-only offenders are non-contact offenders by default - often exposed to CSAM at an early age - and may only become contact offenders after prolonged exposure to CSAM (Broadhurst, 2019).

Differences between non-contact and contact offenders have been identified. These differences align with what we know about online offenders who differ in some psychologically and criminologically meaningful ways from contact offenders. Brown & Bricknell (2018) reviewed recent literature about those that view and collect CSAM. They identified 49 peer-reviewed studies drawing on official criminal justice data about convicted offenders and online convenience samples. CSAM offenders were predominantly white males, tended to be older than the average offender (i.e., between 35 and 45 years of age) but younger, more often single and better educated than contact sexual offenders. Very few had prior offences for contact sexual offences and generally were less likely to re-offend than contact child sex offenders. The evidence also suggested that non-contact CSAM offenders "…tend to be less assertive, less dominant and under-socialized" and "…show higher levels of sexual deviancy than contact or mixed sexual offenders and are more likely to fantasize about children''. The study concluded that the 'profile' of CSAM offenders "...may be different to that of other types of sexual offenders, especially those who commit contact sexual offences against children'' (Brown & Bricknell, 2018, p. 9). CSAM online offenders are better socially adjusted; have less criminal history; and score lower on factors associated with dynamic risk in contact offenders, such as general self-regulation deficits, interpersonal difficulties, and offense-supportive attitudes and

[30] Note this sexual preference is not listed as a paraphilia in DSM-VR.

beliefs (Broadhurst, 2019, citing Babchishin, Hanson, & Hermann, 2011; Babchishin, Hanson, & Van Zuylen, 2015).

Furthermore, online offenders displayed higher sexual deviancy, experienced more psychological barriers to acting on these deviant interests but also exhibited greater victim empathy than contact child sex offenders (Babchishin, et al., 2011; cited in Broadhurst, 2019, p. 317). These psychological barriers may be explained by an avoidance of the emotional attachment of real-life relationships - particularly with children, as this subculture knows that it is "wrong" and they cannot neutralise the problem.

Henshaw, et al., (2020, p. 5) note "...the available research suggests that interventions focusing on sexual and emotion regulation, Internet use and interpersonal skills are likely to be most pertinent to CSAM-only offenders. In contrast, research findings indicate that interventions targeting antisocial attitudes, substance use, general lifestyle instability, and victim empathy are likely to be of less relevance for CSAM-only offenders (Babchishin, et al., 2018; Babchishin, Hanson & Van Zuylen, 2015)".

Building on these insights Henshaw and colleagues outline an offline 10 week Victorian CEP-COPE (Coping with Child Exploitation Material Use) program involving cognitive behavioural and dialectical behavioural group therapy (embedded in acceptance therapy)[31] with the aim of reducing the risk of CSAM offending by supporting the participants in leading "balanced, meaningful lives free of offending". Initiating such a program online is also feasible although we do not yet know if online programs can work to reduce self reported time viewing CSAM or modify offline behaviour or reduce the severity of the CSAM viewed[32]. Two UK prison based treatment programs the i-SOTP (revised and re-titled 'i-Horizon with an individual as well as group counseling component) and Inform Plus (a group based psychoeducation program) provide preliminary support for the need for CSAM specific programs but neither have been evaluated in respect to recidivism. Thus without further research "...accurately identifying the CSAM offenders who are most at risk of subsequent reoffending means that interventions are unlikely to be accurately targeted towards those with the greatest need. This may also result in the over-servicing of many low-risk CSAM-only offenders who do not require any form of treatment, even if specialised programs are available" (Henshaw, *et al*., 2021, p. 10).

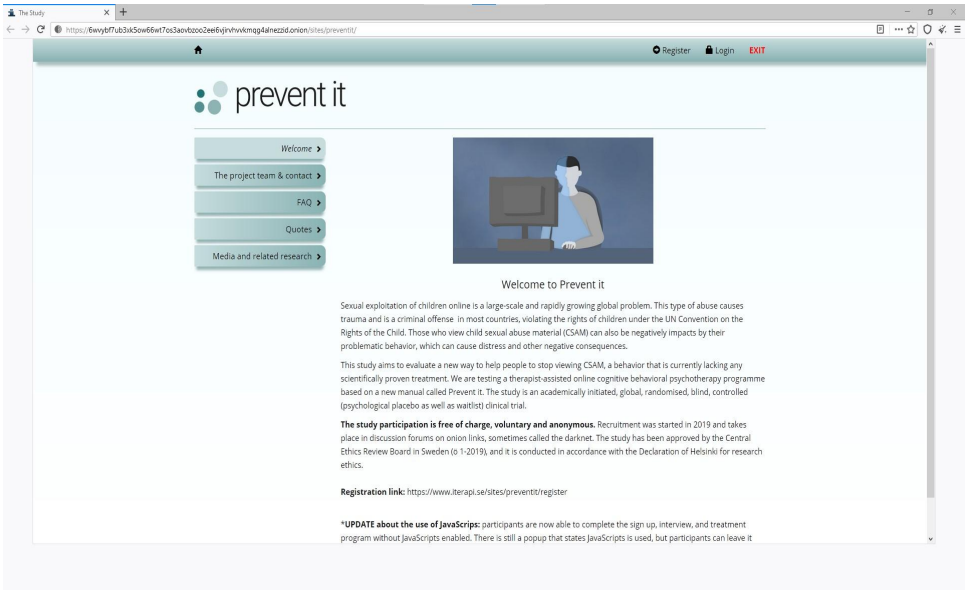
The Swedish *prevent it* online cognitive behavioural treatment (CBT) program operating via a Tor onion service is an example. The program reaches out to relevant Tor CSAM forums to recruit

[31] CEM-COPE focuses on helping participants; understand why and how they offended to identify avenues for intervention and skill development; build and reinforce psychological skills to support desistance; and develop self-management plans based on what they learnt throughout the program, including the identification of ongoing offence specific or broader psychological treatment needs.
[32] Prevent It participants (the first 40) reported a mean time of 7.3 hours a week viewing CSAM, the mean lowest age of the children in the CSAM was 6.2 years and the COPINE severity 7.9, the upper end of the scale.

participants "... who currently access CSAM over onion sites and who would like to stop. Participants must be over 18 years, have accessed CSAM in the week prior to the study's intake interview, have about one hour a week over eight weeks to dedicate to treatment, and be able to read and write confidently in English" (Parks, et al., 2021, p. 1433).

As described, *prevent it* consists of eight weekly modules of discrete content, assignments between modules, and weekly individual therapist feedback. The researchers hypothesized that CBT would be more effective than a placebo in reducing self-reported time viewing CSAM and could also impact on other outcomes including offline offending behaviour, the severity of CSAM, and quality of life. Parks and colleagues argue "...that Internet assisted psychotherapy can be effective for this patient group, as it has been shown to be as effective as in-person therapy for many other psychiatric ailments" (Parks, et al., 2021, p. 1433).

Figure 3: 'Prevent It' an online treatment program for CSAM on Tor (20th September 2021)



Although observation continues and characteristics have been noted, little is known about the CSAM community on Tor. In particular, questions around how this community behaves in conditions of anonymity and in the context of engaging in illegal acts are unanswered. Little is known about how CSAM focused forums influence onion services and vice versa and the extent that users interact with other onion services, forums or platforms.

Online Harm Reduction

Finnish based Protect Children's two-year *ReDirection* project funded by ENDViolence Against Children, asked over 7,000 online users of CSAM about their behavior, thoughts and emotions related to their use of CSAM. Protect Children specialists are developing, in collaboration with psychologists from the Finnish Training Institute of Prison and Probation Service, and researchers

from Police University College Finland the *ReDirection Self-Help Program,* an anonymous rehabilitative program for people who use and distribute CSAM[33].

The preliminary results showed that approximately 50% of the respondents have wanted to stop their use of CSAM but have been unable to do so. A majority, approximately 60% of respondents, have never told anyone about their use of CSAM. Other key findings: a majority of CSAM-users were children themselves when they first encountered CSAM – approximately 70% of users first saw CSAM when they were under 18 and approximately 40% when they were under 13. Additionally, users predominantly view CSAM depicting girls – approximately 45% of respondents said they use CSAM depicting girls aged 4-13, whilst approximately 20% said they use CSAM depicting boys aged 4-13[34].

The monitoring of forums by outsiders can lead to actionable interventions, such as profiling active offenders. Some agencies have explored using undercover law enforcement officers, civil society, or NGO experts (e.g., WeProtect Global Alliance) to promote self-regulation and desistance within these groups.

Devising and implementing effective online interventions for CSAM users requires a multidisciplinary approach informed by close understanding of the incentives and barriers involved in reaching and engaging such a secretive group. The easiest access to the community surrounding CSAM on Tor is through forums. Of the open forums, a support community may present the best opportunity.

An important body of research and expertise has emerged in the past few years from the Australian Institute of Criminology's Child Sexual Abuse Material Reduction Research Program. This offers along with international clinical, policing and cybersecurity expertise a foundation for developing online harm reduction programs that lever the advantages of anonymity.

While there is a lack of research on online treatment of online CSAM offenders (Eggins, et al., 2021), reformed or recovering offenders can also provide counsel to others. Some sub-forums seek to offer education, encourage treatment and reduce harm — usually by focusing on the legal and health issues associated with consuming CSAM, and ways to control urges and avoid stimuli.

Modus Operandi and Crime Prevention

Leclerc, et al., 2021 describe a high-level breakdown of the steps or modus operandi (script analysis) of setting up access to CSAM, consuming and distributing CSAM and engaging related forum or services, while developing a deeper involvement with the CSAM community on the

[33] Personal communications 7/9/21 Anna Ovaska, LL.M., Legal Specialist Protect Children, Finland.
[34] The full report is expected to be released in early October 2021.

darknet. Understanding these step by step processes can point to 'pinch-points' or opportunities for intervention and disruption.

Cale, et al., 2021 undertook a systematic review of 24 studies of the crime commission processes involved in CSAM production and distribution via websites with a focus on the producers of CSAM. The characteristics of offenders are similar to those summarised above but more likely to be contact offenders and most victims report abuse as part of the production. Some producers operate via webcams and do not directly participate in the abuse. Victims as usually known by the offender and a significant proportion of the offenders are family members (see also Salter, et al., 2021). Contact also occurs via online solicitation, grooming and exchange of CSAM as part of the coercive process commonly used by child sex traffickers to manipulate and control victims (Cale, et al., 2021, pp. 6-7). Krone and Smith (2017) found that the production or provision of CSAM, and being an administrator of a CSAM network, were also associated with contact sexual offending.

Discussion

A widely used method for assessing and implementing crime prevention draws on the situational crime prevention approach developed by criminologist Ronald Clarke and many collaborators since the 1980s[35]. Theoretically underpinned by rational choice theory this approach views crime as opportunistic: crime occurs when a motivated offender and an attractive target in the absence of capable guardians converge. While this confluence explains opportunity motivated offenders - offenders also need resources (e.g., skills, knowledge, social capital) to successfully complete a crime and evade detection.

Research on the effectiveness of crime prevention in anonymous digital environments such as Tor is limited. Eggins, et al., (2021, p. 12) systematic review of criminal justice responses to CSAM found a lack of robust evaluations, indeed so scarce as to limit "...the ability to holistically address CSAM offending and operationalise the Australian Centre to Counter Child Exploitation's four pillars of 'prevent, prepare, pursue and protect'".

Edwards, et al. (2021) outlined cyber-strategies relevant to the suppression of CSAM from the perspective of situational crime prevention theory by applying the five main strategies outlined by Wortley & Smallbone (2012). These strategies basically seek to increase the effort required by

[35] See: Sidebottom, A., & Tilley, N. (2017). Situational Crime Prevention and Offender Decision Making. In Bernasco, W, Van Gelder and Elffers, H. [Eds.]. *The Oxford Handbook of Offender Decision Making*, Oxford University Press; Newman, G., & Clarke, R. V. (2016). *Rational choice and situational crime prevention: Theoretical foundations*. Routledge; Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery*. Routledge.; Clarke, R. V., & Felson, M. (2017). Introduction: Criminology, routine activity, and rational choice. In *Routine activity and rational choice* (pp. 1-14). Routledge; Cornish, D. B., & Clarke, R. V. (Eds.). (2014). The reasoning criminal: Rational choice perspectives on offending. Transaction publishers, New Brunswick and New York

offenders by making it more difficult to commit a crime; increase the risk of getting caught; reduce the rewards from crime; reduce provocations to offend; and remove excuses for crime. Opportunities to undermine excuses for CSAM offending, and design new strategies that target "...online situational precipitants (prompts, permissibility, pressure, or provocations" are recommended (Edwards, et al., 2021, p. 2). Some may work even in an anonymous (permissive) platform despite the lack of guardians .

Wortley & Smallbone's (2006; 2012) pioneering application of situational crime prevention approaches to improve the prevention of online sex crimes and the role of conducive environments focused on steps that: disrupt access to offensive websites (increasing the cost, time and effort relative to rewards); improve the identification of victims and offenders (raising the risks of detection); control prompts and stimuli; set behavioral standards (reducing permissibility and removing excuses and neutralisations, e.g., 'just viewing- not touching') and moderating online behaviour by enabling guardians with effective tools (Wortley & Smallbone 2006, pp. 23-29). Newman & Clarke (2013) similarly applied this approach to internet crimes such as online illicit drug dealing, and counterfeit products, noting that as these physical products moved from the virtual to the real world opportunities for detection and disruption occurred but this was not the case with digital products such as malware and CSAM.

Creative research by Prichard, et al., (2021) tested the effectiveness of 'pop-up' warning messages in discouraging individuals from accessing a 'honeypot' website set up on the clearnet offering *barely legal* pornography. 'Pop-up' warning messages did reduce the number of users who continued on the site, especially when warning messages stated that IP addresses could be traced. Messages designed to capture empathy about victims' trauma had less effect. The authors stress the need for more research about the longer term impacts and likely displacement to other safer/anonymous sites. Warning messages about tracing addresses, however, are not likely to work with users of anonymous platforms like Tor.

Messaging intent, platform, incentives, and language (argot) are crucial but little 'market research' to guide pop-up warnings for all types of at-risk individuals/communities and their impacts and duration. Inadequate follow-up may also undermine messaging and impact on their success. As Edwards, et al., (2021; cf. Baines, 2018) note "..a warning message alone does not offer longer term support or assistance for the individual...Including referrals to relevant services as part of the warning message may address this". Edwards, et al., (2021, p. 11) argue treatment clinicians involved in therapy for CSAM offenders could identify the messages that would be most effective along with ways to build access to relevant services.

Attempts at reaching 'hard-to-reach' groups and individuals such as those on Tor if carefully designed could also work but would also need to build a longer term support platform or 'First Aid' online 'hidden' address. Therapeutic treatment and educational strategies have along history in the prevention of sex offender recidivism in correctional settings but internet versions are yet to be developed and should be prioritised, piloted and evaluated.

Conclusion

The risk of child sexual abuse has been amplified by the pandemic and the online epidemic of CSAM challenges the resources and capacities of public agencies such LEA, legal and health services.

Of the anonymous Internet platforms, a critical mass of potential criminals and potential informants of all stripes use Tor. Displacing these users away from Tor could be regressive - especially if they move to E2E encryption services like Signal, Telegram and the like. From an intelligence perspective, the open visibly Tor provides can be advantageous. Australian policy makers need to be aware that they are driving those who know - the major players - further underground.

Policy decisions must consider externalities. Tor uses both public Guard and Bridge nodes and the latter have successfully circumvented the “Great Firewall of China” and its army of censors. Due to the difficulties the anonymity of Tor enables, Internet filtering options (filtering, CSAM and other abhorrent content, drug discussion and violent online extremism, for instance) are likely to displace discussion to digital spaces not affected by the interventions and regulations. Once this material is pushed to the darknet, monitoring of content is much more difficult, and consumption of abhorrent material and radicalisation is more likely to occur.

Clearly the question is: What can the Tor network do to limit or remove abhorrent material such as CSAM? Surely those representing Tor have read complaints in the media, and survivor reports about child sex abuse material. The project has acknowledged the apparent catch-22 it faces, and while it may seem like Tor is avoiding responsibility, the design of the Tor network means that any attempt to moderate the content hosted on its network cannot be achieved without undermining the project itself.

Two responses arise from this conundrum. The first is to recognise the role that Tor plays in national security and law enforcement intelligence and how anonymous platforms such as Tor are used for both noble and criminal purposes. The ‘open-source intelligence’ nature of Tor provides valuable insights into otherwise secretive groups, underground markets and trends. Second, is the potentially positive role of the ‘community’ who use these onion services. This is much more difficult to reason about - partly, because the community is diverse and fragmented - however, there are likely many among this community who could be enlisted in harm reduction and even weaponised to disrupt the ready presence of CSAM on Tor. In the same way that Anonymous fought against the CSAM links on the original Hidden Wiki and against hosting services which allowed CSAM content. Activists have also targeted law enforcement systems that can be vulnerable if not secure and up-to-date.

A better understanding of the networks and communities involved in sharing (viewing), distributing and producing CSAM is crucial to help craft strategies to disrupt and modify them.

Ultimately, law enforcement will *never* be able to de-anonymise all Tor users all the time. It is likely that law enforcement will not be able to de-anonymise Tor users “on demand”.

References

Açar, K. V. (2017). Web cam child prostitution: An exploration of current and futuristic methods of detection. *International Journal of Cyber Criminology, 11*(1), 98–109. https://doi.org/10.5281/zenodo.495775

Arabnezhad, E., La Morgia, M., Mei, A., Nemmi, E. N., & Stefa, J. (2020). A light in the dark web: Linking dark web aliases to real internet identities. *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 311-321. https://doi.org/10.1109/ICDCS47774.2020.00081

Babchishin, K. M., Hanson, K. R., & Hermann, C. A. (2011). The characteristics of online sex offenders: A meta-analysis. *Sexual Abuse*, *23*(1), 92-123. https://doi.org/10.1177/1079063210370708

Babchishin, K., Merdian, H., Bartels, R. & Perkins, D. (2018). Child Sexual Exploitation Materials Offenders. *European Psychologist*, 23(2), 130-143. https://doi.org/10.1027/1016-9040/a000326

Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R., & Hackett, S. (2015). Internet child sex offenders' concerns about online security and their use of identity protection technologies: A review. *Child Abuse Review, 24*(6), 427-439. https://doi.org/10.1002/car.2308

Bouhours, B. & Broadhurst, R. G. (2011). On-line child sex offenders: Report on a sample of peer to peer offenders arrested between July 2010-June 2011. *SSRN.* http://dx.doi.org/10.2139/ssrn.2174815

Broadhurst, R. G. (2019). Child sex abuse images and exploitation materials. In R. Leukfeldt, & T. Holt (Eds.) *Handbook of Cybercrime*. (pp. 310-336). Routledge. https://doi.org/10.4324/9780429460593

Broadhurst, R. G., Ball, M., Jiang, C., Wang, J., & Trivedi, H. (2021). Impact of darknet market seizures on opioid availability. *Research Report no. 18.* Canberra: Australian Institute of Criminology. https://doi.org/10.52922/rr04886

Brown, R., & Bricknel, S. (2018). What is the profile of child exploitation material offenders?. *Trends & issues in crime and criminal justice no. 564.* Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi564

Burgess, M. (2021, September 8). *How Apple can fix its child sexual abuse problem.* Wired. https://www.wired.co.uk/article/apple-photo-scanning-csam

Cale. J., Holt, T., Leclerc, B., Singh, S., & Drew, J. (2021). Crime commission processes in child sexual abuse material production and distribution: A systematic review. *Trends & issues*

in crime and criminal justice no. 617. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04893

Cambiaso, E., Vaccari, I., Patti, L., & Aiello, M. (2019). Darknet security: A categorization of attacks to the Tor network. *Italian Conference on Cyber Security*. http://ceur-ws.org/Vol-2315/paper10.pdf

Canadian Centre for Child Protection (2017). *Survivors Survey - Full Report 2017*. https://www.protectchildren.ca/pdfs/C3P_SurvivorsSurveyFullReport2017.pdf

Clarke, R. V. (1980). "Situational" crime prevention: Theory and practice. *British Journal of Criminology, 20*(2). 136-147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Christensen, L. S., Rayment-McHugh, S., Prenzler, T., Chiu, Y.-N., & Webster, J. (2021). The theory and evidence behind law enforcement strategies that combat child sexual abuse material. *International Journal of Police Science & Management.* https://doi.org/10.1177/14613557211026935

ECPAT International (2017). *SECO manifestations - Live streaming of child sexual abuse in real-time*, Bangkok. https://www.ecpat.org/wp-content/uploads/legacy/SECO%20Manifestations_Live%20streaming%20of%20child%20sexual%20abuse%20in%20real-time_0.pdf

ECPAT International (2018), *Trends in online child sexual abuse material,* Bangkok. https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

Edwards, G., Christensen, L., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends & issues in crime and criminal justice no. 636.* Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78313

Eggins, E., Mazerolle, L., Higginson, A., Hine, L., Walsh, K., Sydes, M., McEwan, J., Hassall, G., Roetman, S., Wallis, R., & Williams, J. (2021). Criminal justice responses to child sexual abuse material offending: A systematic review and evidence and gap map. *Trends & issues in crime and criminal justice no. 623*. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78023

Hannan, S. M., Orcutt, H. K., Miron, L. R., & Thompson, K. L. (2017). Childhood Sexual Abuse and Later Alcohol-Related Problems: Investigating the Roles of Revictimization, PTSD, and Drinking Motivations Among College Women. *Journal of interpersonal violence, 32*(14), 2118-2138. https://doi.org/10.1177/0886260515591276

Henshaw, M., Arnold, C., Darjee, R., Ogloff, J., & Clough, J. (2020). Enhancing evidence-based treatment of child sexual abuse material offenders: The development of the CEM-COPE

program. *Trends & issues in crime and criminal justice no. 607*. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti04787

Karunanayake, I., Ahmed, N., Malaney, R., Islam, R., & Jha, S. K. (2021). De-anonymisation attacks on Tor: A Survey. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2021.3093615

Krone, T., & Smith, R. G. (2017). Trajectories in online child sexual exploitation offending in Australia. *Trends & issues in crime and criminal justice no. 524*. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi524

Leclerc, B., Drew, J., Holt, T. J., Cale, J., & Singh, S. (2021). Child sexual abuse material on the darknet: A script analysis of how offenders operate. *Trends & issues in crime and criminal justice no. 627*. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78160

Lee, H., Ermakova, T., Ververis, V., & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation, 34*, 301022. https://doi.org/10.1016/j.fsidi.2020.301022

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets. In T. Holt, & A. Bossler. (Eds.) *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* (pp. 91-117). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_17

Netclean (2020). *Netclean Report: Covid-19 Impact 2020*, https://www.netclean.com/wp-content/uploads/sites/2/2021/01/NetCleanReport_COVID19_Impact2020_pages.pdf

Owen, G., & Savage, N. (2016). Empirical analysis of Tor hidden services. *IET Information Security*, *10*(3), 113-118. https://doi.org/10.1049/iet-ifs.2015.0121

Owenson, G., Cortes, S., & Lewman, A. (2018). The darknet's smaller than we thought: The life cycle of Tor Hidden Services. *Digital Investigation, 27*. 17-22. https://doi.org/10.1016/j.diin.2018.09.005

Parks, A., Sparre, C., Söderquist, E., Arver, S., Andersson, G., Kaldo, V., Görts-Öberg, K., & Rahm, C. (2020). Illegal online sexual behavior during the COVID-19 pandemic: A call for action based on experiences from the ongoing Prevent It research study. *Archives of Sexual* Behavior*, 49*(5), 1433-1435. https://doi.org/10.1007/s10508-020-01750-7

Prichard, J., Wortley, R., Watters, P., Spiranovic, C., Hunn, C. & Krone, T. (2021). Effects of automated messages on internet users attempting to access “barely legal” pornography. *Sexual Abuse*. https://doi.org/10.1177/10790632211013809

Richards, K. (2011). Misperceptions about child sex offenders. *Trends & issues in crime and criminal justice no. 429*. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi429

van der Bruggen M., & Blokland A. (2021). Child sexual exploitation communities on the darkweb: How organized are they?. In M. W. Kranenbarg, & R. Leukfeldt. (Eds.) *Cybercrime in Context*. (pp. 259-280). Springer. https://doi.org/10.1007/978-3-030-60527-8_15

Suojellaan Lapsia ry / Protect Children's research in the dark web is revealing unprecedented data on CSAM users https://suojellaanlapsia.fi/2021/07/06/suojellaan-lapsia-ry-protect-childrens-research-in-the-dark-web-is-revealing-unprecedented-data-on-csam-users/

Wortley, R. & Smallbone, S. (2006). Applying situational principles to sexual offenses against children. In R. Wrotley, & S. Smallbone. (Eds.) *Situational prevention of child sexual abuse*. (pp. 7-35). Criminal Justice Press. https://www.researchgate.net/publication/29462196_Applying_situational_principles_to_sexual_offenses_against_children

Wortley, R., & Smallbone, S. (2012). *Internet child pornography: Causes, investigation, and prevention*. Praeger, ABC-CLIO, Santa-Barbara Calif.

Wortley, R., Leclerc, B., Reynald, D. M., & Smallbone, S. (2019). What deters child sex offenders? A comparison between completed and noncompleted offenses. *Journal of Interpersonal Violence*, *34*(20), 4303–4327. https://doi.org/10.1177/088626051986923

DeHart, D., Dwyer, G., Seto, M., Moran, R., Letourneau, E. & Schwarz-Watts, D. (2016). Internet sexual solicitation of children: a proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression, 23*(1), 77-89. https://doi.org/10.1080/13552600.2016.1241309

Endrass, J., Urbaniok, F., Hammermeister, L. C., Benz, C., Elbert, T., Laubacher, A., & Rossegger, A. (2009). The consumption of Internet child pornography and violent and sex offending. *BMC Psychiatry, 9*, 43-49. https://doi.org/10.1186/1471-244X-9-43

Elliot, I. A., Beech, A. R., Mandeville-Norden, R., & Hayes, E. (2009). Psychological profiles of Internet sexual offenders: Comparisons with contact sexual offenders. *Sex Abuse, 21*(1), 76-92. https://doi.org/10.1177/1079063208326929

Quayle, E., Jonsson, L. S., Cooper, K., Traynor, J. & Svedin, C. G. (2018). Children in identified sexual images - Who are they? Self- and non-self-taken images in the international child sexual exploitation image database 2006-2015. *Child Abuse Review*, *27*(3), 223-238. https://doi.org/10.1002/car.2507

Krone, T., & Smith R. G. (2017). Trajectories in online child sexual exploitation offending in Australia. *Trends & issues in crime and criminal justice no. 524*. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi524

Seto, M. C. (2017). The motivation-facilitation model of sexual offending. *Sexual Abuse, 31*(1), 3-24. https://doi.org/10.1177/1079063217720919

UNICEF. (2020). *COVID-19 and its implications for protecting children online,* from https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for %20Protecting%20Children%20Online.pdf.

Terbuim Labs (2016) *The Truth about the Dark Web [online]:* https://dsimg.ubm-us.net/envelope/385643/510233/The%20Truth%20About%20The%20Dark%20Web.pdf