Ethical Hacking and the Fight Against Child Exploitation

Jared Young

Professor Carolyn Carvalho

TAS 47999

03/26/25

In a world rapidly merging with the digital realm, technology continues to evolve, offering unprecedented opportunities to drive progress, innovation, and the betterment of humanity. Yet, in the wrong hands, these same advancements can become instruments of unimaginable darkness—tools capable of wreaking havoc, exploiting the innocent, and leaving behind a legacy of destruction that spans generations. Criminals have been using the dark web as a way of circumventing streamline surface-web traceability to perpetuate a longstanding practice of exploiting the innocent for personal pleasure and gain. The anonymity of encryption provided by the dark web used by criminals is also accessible to heroes capable of putting a stop to these predators that thrive on stealing from the weak. With the dark web being one of the primary vessels perpetuating these crimes, there is a dire necessity for law enforcement and ethical hackers alike to come together in ending these crimes altogether. Unfortunately, outdated laws and logistical hinderances often stand in the way of any real progress being made regarding this less discussed topic of online child exploitation. The solution to this fight of internet crimes against children requires a global reformation in terms of modernizing laws and policies, increased international collaboration, ethical hacking partnerships, and utilization of emerging technologies to expedite and empower the current position within the law enforcement industry.

A viable approach in combatting cybercrime is with the same tools used to perform the crime. For instance, the dark web is accessible via a designated web browser called Tor. “Tor enables its users to access the Internet anonymously…[and] hidden services operate only within the Tor network” (Gregory 19). At its core, the way that Tor works can be compared to mailing a friend a letter. You hand the letter to person A to deliver to person B. Person A puts your letter into another envelope before they give it to person B. Person B follows the same steps when delivering to Person C; however, person B only knows how to communicate with person A and C, not between you or your friend. Finally, person C receives the letter and delivers it to your friend who then opens the three-layered envelope and can read the message you delivered. Similarly, the Tor network functions like the three relay characters in the delivery of the letter between you and your friend. Traffic over the Tor network is encrypted three times between a chain of proxy servers that are randomly selected every time a new session is established with the Tor network. This anonymity provided through randomization and encryption is what comprises the dark web at a high-level description for simplicity of the topic regarding cybercrime. “Because Tor attempts to keep users’ IP addresses hidden, the Government cannot rely on traditional identification techniques to identify website visitors” (Gregory 19). Predators can mask their identities behind randomized addressing schemes making it more complicated to identify the true perpetrators carrying on the crime. With the rapid development of the digital landscape, these perpetrators are becoming much more sophisticated in their reach to the desired audience in

delivering this material world-wide. “Livestreaming is on the rise, enabled by connectivity and the availability of inexpensive streaming devices” (U.S. Government 47). Unfortunately, there has been an increase in numbers for these instances especially in the Philippines region. “The majority of identified livestreaming victims live in South-East Asia, in particular the Philippines” (U.S. Government 47). Rising trends and malicious users taking advantage of the technology tools currently in place can only lead one to question what role law enforcement has played in the apprehension efforts towards this sort of deviant behavior in society.

While it would be suspected that apprehension efforts of these criminals would be a top priority to law enforcement, unfortunately there are many outdated policies and practices that hinder the best efforts of police officers trying to pursue these cases in a way that will bring about justice within their communities. When it comes to child exploitation specifically, “The DOJ has issued its strategy only twice—in 2010 and 2016—despite legal requirements to update it every two years” (U.S. Government 35). In a world that is growing technology faster than the legislative bodies can keep up with regulating it, maintaining up-to-date policies and procedures has been a weak point within the Department of Justice (DOJ). Not only is there a lack of attention to revising and updating policies but, “Reports of suspected child sexual exploitation increased 35 percent from 2020 to 2021” (U.S. Government 2). During the peak of the COVID-19 pandemic there was a major spike in reports associated with crimes against children. The increased volume of reporting on top of outdated policy mandates had an unfortunate impact on the victims of child predators keeping them trapped within the confines of their circumstantial conditions, waiting for the help they need to escape. Not all hope is lost within this inconsistency of law enforcement. There are some notable players in this battle such as the Federal Bureau of Investigation (FBI) who worked on a large-scale sting operation to take down a Tor Browser website called ‘Playpen’ under the codename Operation Pacifier. They took a unique approach in that, “Rather than shutting down Playpen, the FBI assumed administrative control…turning it into a honeypot to identify users” (Gregory 25). Using baits to attract criminals in order to identify them, can play a major role in identifying individuals who pose as a threat to innocent children. The statistics behind children who experience some form of sexual abuse or suffer from some form of trauma due to involuntary sexual exposure or experiences is alarmingly high given the rise in reports during the pandemic. As a result of Operation Pacifier the FBI took down, “At least 350 U.S.-based individuals [who were] arrested… [and] 55 American children [were] successfully identified or rescued” (Gregory 26). Some felt that the methodology used by the FBI was not ethical or legal due to privacy infringements, and while “Defendants and privacy advocates bemoaned that the Playpen operation was ‘illegal’ and amounted to dragnet government hacking” (Gregory 27), the actions taken by the FBI still amount to the notion of what behavior is legally and socially acceptable at the expense of the potential impact it can serve for the protection of humanity. While it may seem covert and suspicious to use a fake website to sting pedophiles who are attempting to remain anonymous in their deviant behaviors as they are performing insidious acts in secret, the flip side of using the same anonymity and deception to bring about a justice is infinitely more socially celebrated than the former. These deceptive tactics being used for justice and protection for vulnerable populations brings about a serious question as to what role ethical hacking can play in combatting child exploitation.

Hacking, by definition, is creatively solving a problem or modifying something in a clever or unconventional way. When it comes to cybersecurity, there comes a lot of knowledge and responsibility in understanding just how vulnerable the devices we use every day truly are. There is a massive amount of information that a motivated threat actor can find out about someone just by viewing social media platforms, educational backgrounds, public records, related contacts, etc. All this data is open to the public and available to be

analyzed. Not everyone has the desire or passion to put that much energy into knowing as much as there is to know about everyone on the internet; however, there are digital tools that make that process infinitely more productive and possible. With the developments in Artificial Intelligence (AI) and Open-Source Intelligence (OSINT), extrapolation tools such as Maltego allow you to pull from multiple OSINT data sources and visually see connections to assist with identifying potential suspects or investigating criminal networks. Volunteers can also take part in this activity to identify persons who may be higher risk targets or perpetrators. “Trace Labs works with law enforcement agencies to teach volunteers how to use OSINT tools to find information on missing people and help uncover new leads in both present and past cases through search parties. Trace Labs’ search parties are a good example of how OSINT could be applied and scaled up using crowdsourcing” (Dincelli 7). Trace Labs is one of a few companies that has taken a unique approach to reconnaissance using crowdsourcing as part of the processing power when it comes to getting information to assist law enforcement with investigations. “The goal of the search party is to harness the Wisdom of the Crowd through gamified capture the flag (CTF) events. These events are held at conferences such as Def Con and bring together researchers, analysts, hackers, and other volunteers” (Dincelli 7). This game-like approach is a highly effective way to increase participation and work towards a common goal that equips law enforcement to provide the protection needed within their community. It is a positive feedback loop as the more engagement there is with crowdsourcing, the better law enforcement will be able to protect and serve. While there are many positives to the world of OSINT technology, there are just as many bad actors that also can use this information for malicious purposes. Some privacy advocates worry that large-scale OSINT investigations could violate personal privacy rights and in Ethical Hacking for a Good Cause there are some objective facts to consider:

“There are several learning objectives associated with this teaching case. First, it enhances students’ technical skills that are necessary for becoming cybersecurity professionals. Second, it increases students’ understanding of how technology can be used for the public good and sheds light on the potential for misuse and malicious intent that exists within the same technology. Third, it introduces students to several concepts relevant to information systems (IS), such as OSINT, open-source software, crowdsourcing, and intelligence gathering. Fourth, the case helps students increase their understanding of threats to their personal privacy from publicly available data sources. Finally, the activities in the case will help students better understand ethical issues related to OSINT tools by appreciating that they can be used for productive and nefarious purposes.” (Dincelli 4).

Open-Source Intelligence plays a major role in the early stages of ethical hacking and can provide enough information to recognize vulnerabilities in targets, especially high suspect targets that may contain illegal copies of child content on their devices. Once a potential suspect has been identified through probable cause of possessing any evidence that would be classified as child pornography or sexual content with minors, gaining a warrant to covertly monitor and investigate their internet activity should be permissible under the courts as sufficient evidence for their trial. Using software tools like keyloggers, trojans, spyware, and man-in-the-middle attacks all have the potential to gather the evidence necessary to detail the full extent to which a suspect may or may not have broken the law. With anonymization and encryption being so heavily used for data that is in active transit, data being processed within a live system; however, remains unencrypted:

“Equipped with such malware, or, ‘trojan horses,’ police officers often connect to the Dark Web and install them in suspects’ computers, often those who engage in child pornography, to identify and capture them. But such trojans can also be used more broadly beyond the Dark Web, granting the police a tool to connect

to one's phone, see what the user does in real-time, open their microphone and camera, and potentially extract any data and metadata that is linked to the device. Such actions are commenced remotely without suspicion or action on the user's behalf..." (Haber 26).

Israeli police forces use malware to gain access to suspects' drives, "And as revealed in Israel by a journalist… police hacking on an unprecedented scale in a democratic regime has been ongoing for years under an outdated wiretap law that was never meant to grant such broad access. The Israeli police, as later reaffirmed by a governmental report, systematically used Pegasus, a highly sophisticated and intrusive zero-click malware, against a variety of suspects, sometimes remotely linked to a criminal investigation, under secretive court orders" (Haber 3-4). On the surface, some of these tactics for gaining information may seem intrusive especially for the unsuspecting individual who is conducting criminal acts without the immediate protections for citizens under the Fourth amendment of the United States Constitution. Using this type of malware within an investigation certainly raises some question as to where the line between human rights and privacy exists and to what the proper justification is for breaching that privacy altogether:

"Regulators must oversee that such abilities are not too intrusive and compliant with the legal framework that governs such use. And while there might already be a legal framework to govern police hacking, perhaps mostly under the protection of the Fourth Amendment and the Electronic Communications Privacy Act, it was never crafted for spyware use. As this Article further argues, unlike Frank Easterbrook's famous 'law of the horse' argument, trojan horses must have a specific legal framework that would carefully grant such intrusive powers and delineate its borders, all based upon a proper legal debate on the ways such a framework should be constructed. Policymakers must turn to this discussion today before such police use is normalized, as in Israel and in other countries" (Haber 5-6).

Potentially, there lies no single clear answer; instead, policies need to be implemented that define the legal rules surrounding what type of covert measures are admissible in court for gathering evidence and which methods cross a moral or ethical boundary that does not hold up under the law. Ultimately most criminals will conduct themselves by any means necessary to perpetuate such crimes whether against children, drug trafficking, or espionage alike. As Edward Snowden once said, "Sometimes to do the right thing, you have to break a law" (Brainy Quote). In times where the cost of protecting children from deviant sexual predators comes at the expense of breaking the bureaucratic law, it may be that the resolution does not lie within the hands of law enforcement but under a separate entity still unknown that is complimented by law enforcement. With new and emerging technologies, the solution to this worldwide issue extends far beyond the reach of a single individual and requires a team of advocates who can work together to squelch the darkness that lies within the pits of deviant society.

One of the first changes that needs to be implemented to bring about any change relies on the DOJ to update their strategy to include prosecution efforts for emerging threats such as live-streaming and various encrypted communications that make identifications of perpetrators extremely difficult:

"Producing and sharing child sexual abuse material via apps that support livestreaming and end-to-end encryption is difficult to proactively prevent and even more difficult for law enforcement to catch offenders…an updated strategy could help DOJ prioritize its efforts to address pressing issues such as the increased use of end-to-end encryption—a challenge consistently noted by federal officials we met with during the course of our review" (U.S. Government 31, 38).

In addition to policy changes that need to be made, continued efforts of international communications are going to be critical in the global fight as high numbers of children often go missing and cross international barriers inhibiting their rescue and escape. “The federal government coordinates with international and industry partners and stakeholders… For example, in March 2020, DOJ and DHS, along with government counterparts from Australia, Canada, New Zealand, and the United Kingdom published 11 voluntary principles to counter online exploitation and abuse of children” (U.S. Government 17). With Increased collaboration and law enforcement policy efforts, these regulations could be extended to include ethical hacking partnerships that span internationally and include legal protections similar to the “Good Samaritan Law” which protects those who provide CPR should any health conditions result from the lifesaving efforts of the provider. Any ethical hacking attempt made in good conscience for the protection of a child should result in the prosecution of the perpetrator and not the individual who used the resources necessary to bring about a justice within society. By encouraging these sorts of widespread hacking partnerships, community-sourced intelligence gathering will mitigate the stigma surrounding ethical hacking and allow for increased involvement throughout the community with the use of OSINT technology to bring about the answers to cases sooner than later. “Cybersecurity professionals, law enforcement agencies, and volunteers from nonprofit organizations utilize OSINT to address various societal challenges and crimes, including environmental crimes and abuse, human rights violations, child exploitation, human trafficking, and domestic violence" (Dincelli 15). Lastly, it is critical that despite all best efforts in collaboration and policy changes, keeping up with the fast-changing landscape of emerging technologies will be the backbone in propelling investigations and expediting the recovery process. Using AI in addition to OSINT will be ground-breaking given the speed and processing power at which these means can calculate and reason through data when specializing in scraping resources for personally identifiable clues or data that can lead to identification of suspects or victims:

"OSINT tools are useful for performing various cybersecurity-related tasks, such as penetration testing, vulnerability assessment, network analysis, threat intelligence, incident response, and identifying potential threat vectors, among other uses..." (Dincelli 14).

Not only will AI assist with OSINT data processing, but it will also assist in the forensic process after the evidence and data has been collected. Processing through a hard drive with images and videos will become much faster and easier as the technology improves. In addition to hard drive analysis:

"The DHS Science and Technology Directorate developed SpeechView, which uses machine learning to analyze and translate audio content in videos. SpeechView greatly increases the productivity of investigators by translating and transcribing audio content into a searchable format so it can be reviewed and analyzed quickly" (U.S. Government 31).

With the assistance of technology being accessible to law enforcement, it will greatly improve the efficiency at which cyber-related incidents can be processed and potentially enhance the overall outcome of the investigation. The problems faced today with limitations in laws and disconnection from technology within law enforcement can be solved with the greater implementation of emerging technologies such as AI and OSINT in the recovery of oppressed and abused individuals who are suffering in silence. Without a multifaceted and multilayered approach to this social dilemma, there will never come about a solution. It will require education, law enforcement, government agencies, parents, technology enthusiasts, and members of society who wish to join the fight as one. The sheer potential that lies within each part of the leading bodies performing their own specific role will transform the nature of this beast from something big to

something small.

As stated by Thomas Szasz, “If he who breaks the law is not punished, he who obeys it is cheated. This, and this alone, is why lawbreakers ought to be punished: to authenticate as good, and to encourage as useful, law-abiding behavior. The aim of criminal law cannot be correction or deterrence; it can only be the maintenance of the legal order.” (Crime and Justice). The presence of the dark web will always exist and the difficulties that come from identifying individual users via the traditional methods used on the surface web will always be the struggle that it currently is. Capturing the perpetrators will require a sophisticated series of traps and malware that appear as though they are one of the illegal sites to lure suspects out of hiding. Some traps include honeypot sites that look and appear as though they are a legitimate site while collecting potentially identifying information on the visitors of that site. While there are many laws inhibiting this due to outdated policies and the rapid development of emerging technologies, it is increasingly difficult for law enforcement to uphold more efficient measures to protect the community due to the lack of legislature surrounding these new methods of gathering evidence. Ethical hacking can play a major role in gathering warranted evidence from suspected individuals without alarming them that they have been caught. The evidence gathered from a backdoor monitor on their system can lead to undeniable evidence that would then lead to their prosecution and ultimately their incarceration. Through crowdsourcing events and ethical hacking partnerships regulated under an umbrella of privacy protections as for other citizens, there is a huge potential for groundbreaking process changes when it comes to the investigative process. Malware and AI analysis tools can aid law enforcement in quickly analyzing and determining actions to be taken against individuals suspected of distributing or possessing child pornography on their devices. By modernizing laws and expanding ethical hacking programs, the fight against child exploitation can be mitigated significantly through the continued efforts of those advocating for the innocent in need.

Works Cited

“Crime and Justice:” Crime and Punishment - Quotations, www1.udel.edu/CRJU/dgulick/quote.htm#:~:text=If%20he%20who%20breaks%20the,who%20obeys%20it%20is%20cheated. Accessed 22 Mar. 2025.

Dincelli, Ersin, et al. “Ethical Hacking for a Good Cause: Finding Missing People Using Crowdsourcing and Open-Source Intelligence (OSINT) Tools.” Communications of the Association for Information Systems, vol. 53, July 2023, pp. 1052–71. EBSCOhost, https://doi-org.proxy.library.kent.edu/10.17705/1CAIS.05345.

“Edward Snowden Quotes.” Edward Snowden Quotes, Brainy Quote, www.brainyquote.com/quotes/edward_snowden_765226. Accessed 22 Mar. 2025.

Gregory, Whitney J. “Honeypots: Not for Winnie the Pooh but for Winnie the Pedo: Law Enforcement’s Lawful Use of Technology to Catch Perpetrators and Help Victims of Child Exploitation on the Dark Web.” George Mason Law Review, vol. 26, no. 1, Fall 2018, pp. 259–312. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&AuthType=ip&db=lgh&AN=13906830&site=eds-live&scope=site.

Haber, Eldar. “The Law of the Trojan Horse.” U.C. Davis Law Review, vol. 57, no. 3, Feb. 2024, pp. 1667–720. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&AuthType=ip&db=lgh&AN=17615939&site=eds-live&scope=site.

U.S. Government Accountability Office. GAO-23-105260, Online Exploitation of Children: Department of Justice Leadership and Updated National Strategy Needed to Address Challenges. U.S. Government Accountability Office, 2022