Gyancity Journal of Engineering and Technology,
Vol.10, No.2, pp. 1-28, July 2024
ISSN: 2456-0065 DOI: 10.21058/gjet.2024.102003

Cybersecurity, data science, and modern slavery "human trafficking"

Waheeb Abu-ulbeh
Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine
w.abuulbeh@pass.ps

Abstract

Research and first-hand evidence shows that technology is being abused by human traffickers during all stages of this crime, including recruiting, controlling, and exploiting victims by harnessing technology by traffickers. As the world continues to digitally transform, internet technologies are increasingly being used to facilitate this crime, and with the advent of new technologies, some human traffickers have adapted their modus operandi to cyberspace by integrating technology and leveraging digital platforms to advertise victims, and recruiting and exploiting them. Despite its frequent misuse, technology can be a source of strength for participants in the fight against human trafficking through a wide range of technological tools that can be used to support their efforts in combating human trafficking. Human traffickers have subjugated the digital society and exploited vulnerable individuals, especially children, for illegal purposes so that the internet has become an ideal space for this type of crime, providing countless opportunities for interaction between human traffickers and victims. This study sheds light on the role of data science and cybersecurity in combating this criminal phenomenon through a review of the various technological solutions and tools available in this field on the Internet.

Keywords: *human trafficking, digital transformation, cyberspace, data science, cybersecurity.*

1. Introduction

As technology and digital literacy continue to accelerate and grow exponentially in many directions around the world, the advantages and disadvantages associated with these assets are following suit, and innovation and technological transformation are now helping to facilitate communication and discourse between individuals from around the world, reaching wider audiences despite long distances and large time zones.

The internet is a virtual reality in which almost anything can happen, and the digital world is certainly useful in many ways, including but not limited to: easy access to a wide range of information, space for collaboration between parties in the private and

public sectors, and a way to acquire knowledge and education without having to waste huge sums. The development of information and communication technologies that facilitate access to them through smart phones and the Internet has an important influence on the emergence of various types of crimes, including the crime of human trafficking, and although technology is often misused to facilitate human trafficking, its positive use can also help practitioners in combating this crime. With this in mind, future success in eliminating human trafficking, in its many forms, will depend on how countries and societies are prepared to harness In its responses and processing to it, human trafficking can be defined as "a highly misunderstood crime." People don't often realise that human trafficking is mostly done online," Jones said. "There doesn't have to be movement for trafficking to happen. People can be trafficked and still go about their daily lives (Julie Jones, the founder and CEO of Human Intell. Services, Canada), and the overlap between cybercrime and human trafficking flourished during delinquency. From finding and grooming vulnerable people via social media apps to promoting and soliciting their bodies on the dark web or through encrypted channels.

The importance of the study

The importance of the study can be seen as theoretical and practical; The subject of human trafficking is old, and the introduction of technology in the stages of its completion in the modern era has become the subject of interest to many researchers, as these technological means and tools are relied upon to find effective solutions to combat this phenomenon, reduce its effects, and address many problems and challenges facing the security of societies and human rights.

The practical importance of the study is highlighted by the fact that it provides a source for subsequent studies on the subject of human trafficking in Arabic websites and forums, which are relatively few compared to other topics, especially with regard to the use of technology and its relationship to human trafficking and facilitating its mechanism and the use of technology as well as to develop countermeasures in anti-human trafficking operations.

It also draws the attention of the public and private sectors and professionals to the importance of the current study in that it will clarify the basis of the requirements that organizations must take to ensure that technology is not misused and the problem worsens.

Study problem

This research highlights the importance of the relationship between technology represented in data science, cybersecurity and the phenomenon of human trafficking, and the study also examines the available technological models that are used to facilitate the commission of this crime, and based on the above, the main question of the study: What is the relationship between the spread of modern technology and the phenomenon of human trafficking?

The study will also answer a set of sub-questions, which are as follows:

- What are the negative effects of the misuse of technology on the spread of human trafficking?
- What techniques and technological methods do human traffickers use in committing crime?
- What is the role of data science and cybersecurity in combating human trafficking?
- What is the role of the public and private sectors to be victims of this crime?

Study methodology

This study is based on the descriptive and analytical approach to the role played by data science and cybersecurity in combating human trafficking, by examining the literature on the Internet, and this study seeks to provide a guide to the existing technologies and technological solutions that help in the spread of this crime and on the other side in combating it, and the most important challenges and possible opportunities in this field.

2. Overview of trafficking in persons and smuggling of migrants

Trafficking in persons is a combination of three elements: act, means and purpose. It is defined in article 3 of the Protocol against Trafficking in Persons as:

"The recruitment, transportation, harboring or receipt of persons by means of the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or exploitation of a situation of vulnerability, or by giving or receiving payments or benefits to obtain the consent of a person having control over another person for the purpose of exploitation. Exploitation includes, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor, forced service, slavery, slavery-like practices, servitude or the removal of organs."

Cybercrime, trafficking in persons and smuggling of migrants have a key common denominator: they represent lucrative activities for organized criminal groups that stand ready to profit from them, regardless of the effects on victims of trafficking in persons or migrants who risk their lives and pay with their lives to escape violence and conflict.

In more developed countries, the ubiquitous proliferation of smartphones among the child and young adult populations has led apps to play an increasingly important role in the exploitation of young victims. Apps often have the ability to track GPS, allowing traffickers to track the physical location of potential targets, and teenagers-focused social apps encourage unwise interaction and disclosure of private information, often without any verification of the other party's identity. In the process of communication. ((unodc.org), 2021)

Social media, cryptocurrency, dark web

As technology continues to evolve, experts are calling for more education for law enforcement officials on the role of social media, dark web, cryptography, and

cryptocurrencies in human trafficking practices, specifically on how to facilitate crime and the evidence needed to prosecute human trafficking crimes.

This starts with understanding the types of websites:

- Surface Web: Internet zones accessible by search engines, available to the general public using standard search engines and accessible using standard web browsers that do not require any special configuration (such as Mozilla Firefox,Microsoft's Internet Explorer,and Google Chromeranging from 2 to 10 percent of the data is online.

- Deep Web: Internet zones that can be accessed through a database (which can be accessed through search engines). Many deep web sites consist of data and content stored in databases that support the services we use daily (such as social media or banking sites); they contain about 90% of the data online.

- Dark Web: Internet zones that cannot be accessed through regular search engines or deep web sites; It relies on communications between trusted peers and requires access to specialized software, tools, or equipment. Two common tools for this purpose are Tor andI2P, which are commonly used to provide anonymity, once logged into Tor or I2P, the most direct way to find pages on the dark web is to receive a link to the page from another user; consisting of 0.01 percent of the Internet.

3. Misuse of technology by traffickers

Research and first-hand evidence shows that technology is abused by human traffickers during all stages of crime, including recruiting, controlling and exploiting victims through some of the main reasons for harnessing technology by traffickers include:

1. Anonymity. Perpetrators and their accomplices communicate through encrypted apps or use the dark web to connect. Victims are recruited through fake social media accounts and fake profiles on apps. In addition, cryptocurrencies allow traders to conduct financial transactions and transfer criminal proceeds anonymously (Europol, 2016).

2. Facilitate the recruitment and exploitation of victims by traffickers. Through online interaction and targeting potential victims, access to personal data, arranging logistics and transportation, and recruiting through social media.

3. Facilitate transactions and expand the market. Misuse of technology can also make it easier for traffickers to engage in transactions with users, enter new markets and expand criminal operations. For example, with regard to trafficking for the purposes of sexual exploitation, technology - especially the Internet - helps traffickers to advertise victims and communicate more easily with a large market of users. In addition, large online platforms that host advertisements Sex services for sex traffickers have the means to attract customers, thereby sexually exploiting victims. The trend is

upward, as online advertising of sexual services is an increasing phenomenon related to sexual exploitation, with children being advertised as adults.

4. Expand the means by which victims can be controlled and exploited. Misuse of certain technologies can also help traffickers control and coerce victims. For example, traffickers may use GPS software. In phones to track the movements of victims, or in the case of domestic slavery and other forms of labor exploitation, monitor and control victims through video surveillance. (OCSE, 2017).

5. Evolution of Internet platforms used

Analysis of court cases indicates the presence of the use of various Internet platforms by traffickers. Three broad types of platforms have been identified:

- Social media, including Facebook, Myspace, Skype andWhatsApp.
- Classified webpages for advertisement refer to public websites where individuals post advertisements or browse items or services to buy or sell;
- Free-standing webpages refer to websites created by merchants that are not part of larger domains.

6. New geographic areas for trafficking in persons

Internet technology has expanded the geographical reach of traffickers' operations, the Internet helps traffickers operate across borders and in multiple locations at the same time, while physically exploiting victims in one place. By leveraging Internet technologies, traffickers are able to overcome geographic distances by using "cyberspace" to connect themselves, victims and end consumers of exploitative services. This type of trafficking may or may not require the transfer of the victim, although some cases have shown that victims can be moved between States.

Cyber flows are often characterized by detaining victims and forcing them to perform video presentations, allowing perpetrators to connect with potential customers living abroad. This type of trafficking has been recognized in many countries and usually relies on the availability of video equipment and digital recording devices to broadcast the exploitation of victims. The cases examined did not describe many cases of cyber flows. It seems that those reported are large in terms of the number of victims and agents. Internet technologies allow exploitation in front of larger audiences than is generally possible in the case of traditional trafficking.

UNICEF reported on how children can be at greater risk of exploitation in front of webcams – communicating with abusers residing elsewhere and, in many cases, without their parents' knowledge. (UNICEF, 2017) While this does not constitute trafficking per se, it describes how offensive material is used and can be easily disseminated through digital tools, connecting victims and perpetrators in cyberspace.

Cyber traffickers: The way in which Internet technologies are used to commit trafficking crimes in persons changes according to the profile, group size and level of "cyber expertise" of the traffickers themselves, most cases of trafficking facilitated by

the Internet take place on a small scale, and for trafficking that occurs offline, lone traffickers can assert control over their victims in several ways. Analysis of cases before the court reveals said that traffickers working alone online generally recruit and exploit their victims in their countries of residence, and of the 35 cases in the dataset involving a single online store, only six involved the international transport of victims.

Cyber experts: Traffickers may have different levels of computational literacy, some of whom use unsophisticated Internet-based technologies. For example, several trafficking cases for sexual exploitation reviewed by a smartphone with a camera have been committed. Sophisticated technologies allow traffickers to expand their activities, and it has been documented that organized criminal networks have attempted to recruit hackers or cyber experts to support their operations.

4. Strategies used for human trafficking: how it works

The reviewed court cases highlight two distinct types of strategies: one in which traffickers proactively look for a specific type of hunting victim and the other where traffickers attract potential victims to fishing. (Processo nº 2004.81.00.18889-0 (unodc.org), 2007)

Hunting strategies

Traffickers may proactively target specific victims or customers in a strategy that can be referred to as "sniping", which uses sniper strategies to reach victims and establish contacts with potential buyers of exploitative services.

In this approach, traffickers' targets are not random, but are chosen based on specific characteristics, such as economic, emotional or other vulnerabilities, which therefore make them more vulnerable to exploitation or abuse.

Fishing strategies

Conversely, fishing strategies involve traffickers posting advertisements online and waiting for a response from potential customers or victims. In one case, traffickers used fake profiles on a social media platform to advertise modeling jobs in a foreign country, and eventually, traffickers sexually exploited women who were deceived by the ads, and in this single case, nearly 100 women were recruited through hunting strategies.

Misuse of technology has been exacerbated by a number of enabling factors such as:

1. Inadequate legal frameworks: that do not provide the tools to enable successful investigations and prosecutions to combat online impunity or to efficiently use the full toolkit to combat trafficking in persons in the online world;

2. The transnational nature of human trafficking: facilitated by ICTs where perpetrators, victims and technology platforms can be located in different countries, generating additional challenges in terms of jurisdiction, evidence collection, extradition and mutual legal assistance;

3. Weak local and international cooperation: between government institutions and the private sector, which hinders opportunities to respond quickly to innovative approaches adopted by traffickers and does not allow full use of available resources and expertise in various sectors;

4. Lack of capacity, awareness and experience: among law enforcement, prosecutors and the judiciary due to, among other factors, the complex and evolving nature of ICT-facilitated trafficking;

5. Limited availability of technological tools: (as well as the necessary expertise and capabilities) for anti-trafficking personnel.

Using technology to combat human trafficking

Despite its frequent misuse, technology can be a source of strength for participants in the fight against trafficking in persons, government authorities, non-governmental organizations, international organizations and private sector companies have a wide range of technological tools that can be used to support their efforts in combating human trafficking. A number of initiatives have already been launched around the world on the use of technology to combat human trafficking.

For example, the Technology Against Trafficking Coalition, a coalition of technology companies working to combat human trafficking and with the support of various stakeholders including international organizations such as the Organization for Security and Cooperation in Europe and the International Organization for Migration, has developed more than 260 technological tools that support anti-trafficking work. (bsr.org, 2019)

One of the technological methods used in this field

- Data collection and analysis: The online world has no borders, and tens of thousands of websites, chat rooms, apps and online video games, among other things, can be linked to criminal human trafficking enterprises. Since it is impossible for law enforcement authorities and NGOs in any country to monitor and analyze everything in the online world, Various authorities, technology companies and NGOs use data tools to compile and synthesize relevant information into useful reports and thus provide valuable resources; and enable various capabilities in digital forensics on the Internet, cryptography, and other areas (Nepal Failing to Protect Women from Online Abuse, 2020) (Thailand Toughens Rape Laws, 2019). Investigations impede privacy laws that make it difficult to monitor and arrest perpetrators. Multinational tech companies, such as Google, Microsoft and Facebook, are collaborating to develop digital tools and help law enforcement combat them.

- Training and Education: Teaching the dangers of online chat to children is important to reduce the risk of becoming a victim of online sex. Through online chat, the fraudster may gain knowledge about the child's hobbies and favorite things by following his page or waiting to see what the child posts, after the predator acquires this personal knowledge, he continues to talk to this child, pretending that he is also a

child with the same interests to entice them after gaining their trust. This involves the risk of because the child may never know who is on the other side of the screen. For example, the Malaysian Ministry of Education has introduced awareness of online trafficking in secondary school curricula.

- Blockchain technology: for tracking and source. A large number of private sector companies are taking measures to identify and mitigate the risks of human trafficking in their global supply chains. Since global corporate brands have tens of thousands of suppliers spread across the globe, monitoring supply chains is a very complex process.

- Artificial intelligence: The computational power of AI and machine learning is increasingly being leveraged to combat many traditional challenges, including human trafficking. AI can help make predictions, recommendations, or decisions independently and without human intervention. In the context of human trafficking, examples include the use of AI to determine what a child victim of sex trafficking will look like as an adult, to enable autonomous automated communication with potential users of services who are victims of trafficking. To identify the features of hotel rooms where victims may be held, and to identify financial transactions that may indicate the existence of human trafficking networks;

- Facial recognition: Visual processing software can be used to search for images and videos of trafficked victims. Facial recognition technology can be used in web crawling to search for photos and videos of trafficked victims. This type of technology can also help law enforcement authorities analyze tens of thousands of photos and videos to identify content attributed to a specific individual.

- Technology for victims and survivors: A number of technology-based tools have been developed to identify or support victims and survivors, such as applications that allow educators to interview potential victims in different languages or e-learning platforms to teach survivors new job skills. In the context of labor exploitation, technological solutions based on online surveys, SMS and voice-activated applications are used to engage workers at scale to request information about practices. Potential exploitative across multiple levels of supply chains.

6. Ethical considerations and data protection

The increasing use of technology to combat human trafficking has highlighted considerations around data privacy, ethics, transparency, accountability, and consent. Most applications of technology to combat human trafficking require some form of data collection, storage, sharing, and analysis—each of which has its own inherent risks and requires well-established protocols and protections, including:

- Ensure that any data, especially information that identifies a person, is stored securely and that only authorized people have access to it.

- Establish gender- and age-sensitive consent protocols.

- Assess the risks of information released by law enforcement authorities that could be linked to the identities of victims, potentially putting them or their families at risk;
- Ensure that data obtained from victims and vulnerable people is used to help them and end exploitative practices, rather than to advance commercial interests; Ensure that data shared between relevant agencies and between countries is in accordance with national and international legal frameworks and takes into account privacy and confidentiality standards;
- Address potential conflicts between the need to protect anonymity and confidentiality and the need to support victims of trafficking in accessing services or rehabilitation.

Digital statistics for the crime of human trafficking: There are no accurate statistics on human trafficking in the Arab world, and to understand the technology used practically in combating human trafficking, we will look at the experience of the United States of America in this field.

- **Human trafficking (USA model)**

U.S. The following statistics come from the web page of the Polaris Project, a non-profit organization that fights to end the resurgence of human trafficking worldwide and which operates the National Human Trafficking Hotline. It is important to note that despite the validity of the data and the most accurate representation available, there are countless cases of human trafficking that are never reported and never detected. The true number of cases is likely to be much higher than what is now recorded and described here; however, the dark form of the crime prohibits the possibility of full disclosure. The 2019 data report identifies 22,326 victims and survivors of human trafficking, and of these, 14,597 (nearly two-thirds) were victims and survivors of sex trafficking. The report additionally identifies 11,500 trafficking cases and 4,384 traffickers.

The United States' Response to Human Trafficking the United States has initiated and implemented several bills and laws aimed at combating human trafficking and its harmful and persistent effects, which are arguably the most successful. Trafficking Victims Protection Act the United States Congress passed the Trafficking Victims Protection Act (TVPA) in 2000,

The role of technology in facilitating human trafficking in the United States: As the use and reliance on technology increases in the United States, the potential for misuse when placed in the hands of the wrong individuals increases. Human traffickers have subjugated the digital community by using both the surface web, the visible web available to the general public, and the dark web, which requires special authorization to access, and exploiting vulnerable individuals, especially children, for illegal purposes. The online arena has become ideal for this type of crime, providing countless opportunities for interaction between human traffickers and victims. From popular social media icons, such as Twitter and Facebook, to commonly use advertising sites,

such as eBay, traffickers manipulate and deceive users on a massive scale on these platforms. Classified ads have become a marketing method and a supply and demand tactic. Initially, ads are used to lure victims with false promises, and then, once they are obtained, they are used to lure victims with false promises.

Hire buyers online

Once victims have been successfully discovered, manipulated and captured, traffickers are tasked with creating the perfect online classified ad to showcase their supplies to desired potential customers. Technological advances have made this simpler as clients can now interact with commercial sex actors through digital cameras, webcam footage and online chat rooms. Webcam sex is particularly dangerous because it can lead to transnational exploitation, as the footage can be seen all over the world at any time. In addition, this type of commercial sex is often supplemented by live streaming, making it easier for criminals to escape the blocking and censorship tools that law enforcement officials put in place to detect and monitor child pornography and child exploitation online. Webcam sex is not usually recorded, so the possibility of leaving a digital footprint behind is highly unlikely. Monitoring is limited (Barney, 2018).

The role of technology in combating human trafficking in the United States

Fortunately, technological advances and developments can also be used positively to combat and reverse their negative effects. Functional cybersecurity measures and initiatives used by law enforcement are highly effective in controlling, preventing, and ending this pandemic. To better understand the scope and extent of law enforcement officials' use of technology in the digital world to address online sex trafficking, most of the information law enforcement officials use to detect and resolve sex trafficking cases involves the application of open source intelligence, which is often referred to by the acronym OSINT and Open Intelligence. The source refers to information that is publicly available to everyone and can be accessed without restriction or limitation, in most cases (Vosler, 2020). While the drawback of using OSINT in an investigation is the sheer volume of data that law enforcement must examine, it is beneficial because all one needs to access this wide range of information is a computer, an Internet connection, and the strategies and skills needed to access this range. Wide range of information.

Categories of Open Source Information When conducting open source intelligence analysis during an investigation, cyber analysts often deal with four different types of information: OPEN SOURCE DATA (OSD), OPEN SOURCE INFORMATION (OSINF), OPEN SOURCE INTELLIGENCE (OSINT), and VALIDATED OPEN SOURCE INTELLIGENCE (OSINT-V).

The next step, after analyzing the ad descriptions, is the images themselves.

As previously mentioned, investigators will look at height, weight, and health status to determine if the person in the photo is a minor and will look at any photo that is grainy or censored. Investigators must find somewhere else on the Internet where these

images exist, and the OSINT framework has the ability to do this. Reverse image search can be used to find images similar or related to those being analysed by investigators.

Reverse imaging can help connect ads on different platforms using the same images. Additionally, if a trafficking victim's family reports them missing, their photo may appear in a missing persons ad or flier, which can strengthen the investigation and put a name to the table. Agencies often release photos of the victims in these ads to the public to see if anyone recognizes them or knows who they are. Unfortunately, most of these victims disappear or leave under inauspicious circumstances and do not have family or friends who care enough about their disappearance, which makes the investigator's job even more difficult. In these cases, biometric facial recognition can be useful for making cross-platform matches.

Biometric identification and segmentation

Hashing is the production of a number created from a text string and is another cybersecurity technique used in sex trafficking cases, as it can be used to facilitate faster file comparisons. The three most common hash algorithms are MD5, SHA1, and SHA 256. A hash produces unique values for pieces of data or assigns a number to a file or message of some type. Agencies, such as the Internet Watch Foundation, create hashes of child exploitation images and create a comprehensive list of hashes to share with other agencies. The list is placed in digital forensics software that has the ability to scan the device's hard drives for suspects and compare data. Retail saves law enforcement a lot of time, money, and resources that they may not have available to them in sex trafficking cases.

The digital world meets the physical world

Once sex trafficking ads are identified, analyzed and verified, law enforcement moves to the next step, which combines the physical and digital worlds. Using the information they have gathered in the digital world about the trafficker and the trafficked victim, law enforcement attempts to set up meetings in the physical world with these individuals .

US Department of State Trafficking in Persons Report 2023

The US State Department's 2023 Trafficking in Persons Report highlights a new form of human trafficking that has gone largely unnoticed outside victim support circles but which has serious implications not only for ending the scourge of human trafficking but also for... Cybercrime, online romance, cryptocurrency, and other scams go back decades, but the COVID-19 pandemic has pushed the pivot toward the widespread use of human trafficking to commit these crimes.

Question 1: Why has the online fraud industry grown so rapidly in the past three years, and why are trafficking victims used to commit fraud?

Before the COVID-19 pandemic, holiday towns and special economic zones in Southeast Asia were hosting a massive influx of citizens, including a few who exploited local corruption to grow large-scale criminal enterprises. Hotels, online and physical

gambling operations flourished, but so did prostitution, violence and online fraud. Online scams are traditionally difficult to track - especially cryptocurrency scams. The cyber fraud industry's shift towards human trafficking began when Cambodia's ban on online gambling in 2019 significantly reduced casino and hotel revenues and depressed property prices. In casino cities in Southeast Asia. In 2020,

Question 2: What is the scale of the problem, and how are victims recruited and trafficked?

The COVID-19 pandemic has fueled economic desperation that has made people more vulnerable to trafficking, and although it is difficult to know with certainty how many people have been trafficked for fraudulent purposes, the Office of the United Nations High Commissioner for Human Rights (OHCHR) It was estimated that the number reached 100,000 victims.

As with many forms of human trafficking, traffickers posing as recruiters post fraudulent job opportunities on Facebook, Telegram, and job sites. But unlike other traffickers, the scams target educated victims with exploitable skills — such as English or Chinese language proficiency or a technology background — and promise attractive salaries for jobs in customer service, information technology, computer programming, and related industries. Fraudsters usually pay for the workers' travel costs, but upon arrival, they confiscate the victims' passports and demand that the victim pay their "debt." This coercion is often accompanied by physical and sexual abuse, restrictions on movement, and starvation. Some female victims are also forced to act as models in video chats with potential fraud victims or forced into sex work if they cannot meet their fraud quotas.

Q4: How is this problem addressed?

Many traditional anti-trafficking strategies are deployed to prevent and punish those who recruit victims into online scams.

- Preventing Fraudulent Recruitment: Multiple countries, including the United States, have issued warnings to their citizens about the dangers of being lured abroad by misleading online job advertisements, especially poor job offers in the technology sector with suspiciously high wages.

- Suppression of fraudsters: shutting down scammers Preventing online scams and dismantling the criminal enterprises that profit from them would reduce demand for trafficked workers. While tech companies like Match Group and Meta have already taken steps to raise awareness and remove suspicious posts, Efforts to date have not been sufficient to eliminate the scale of these online scams.

- **Human trafficking (Canada)**

Canada is actively combating this issue at the national and provincial levels. Law enforcement agencies, justice partners, non-profit organizations and various community groups across the country are working collaboratively to improve awareness and early recognition of trafficking, to protect and support trafficking

survivors, and to investigate and prosecute trafficking crimes. The primary focus is now on interagency communication, cooperation, and intelligence sharing, as well as multijurisdictional investigations and prosecutions.

In September 2019, the federal government presented its $75 million National Human Trafficking Strategy. It adopts the National Strategy to Combat Human Trafficking on Canada's strategic efforts to prevent and respond to gender-based violence, including implementation of the National Inquiry into Missing and Murdered Indigenous Women and Girls' Calls for Justice.

Its strategy also allocates funding to the Canadian Human Trafficking Hotline, a 24/7 multilingual service that connects callers to support and services, which launched in May 2019. During its first year in service, 2,390 substantive references were sent to the service, including calls, emails, online chats, and web forms, and it successfully identified 415 cases of human trafficking. The country is taking a victim-centered approach to this issue, and based on the internationally recognized pillars of prevention, protection, prosecution, and partnership, Canada is also the first country to incorporate a new pillar of "empowerment" in an effort to enhance support and services for victims affected by this crime.

In this regard, the Canadian government stressed that law enforcement should be comprehensive in investigating all cases of online traffic. If more criminals are arrested and sentenced to more stringent penalties, fewer people will be motivated to participate in online sex trafficking rings. Therefore, law enforcement must invest more resources, for example, in technology and experts who can track criminals, even when they are pursuing criminals. They hide their location.

Data science and human trafficking

Human trafficking is a modern form of slavery that involves the exploitation of people for the purposes of forced labor, sexual exploitation, or other forms of exploitation. It is a global issue that affects millions of people every year, including women, men and children. On the other hand, data science is a field that involves using statistical and computational methods to extract insights and knowledge from data. The intersection between human trafficking and data science can be a powerful tool for identifying and combating human trafficking. By leveraging data science techniques, law enforcement agencies and other organizations can better understand the patterns and characteristics of human trafficking, which can help them identify and arrest victims. Traffickers. Specific ways in which data science is used to combat human trafficking include:

1. Data Collection and Analysis: One of the main challenges in combating human trafficking is identifying victims and traffickers. Data science can play an important role in this process by collecting and analyzing data from different sources. For example, law enforcement agencies can collect data on known trafficking cases, such as the age, gender, and nationality of victims, the location of trafficking, and the methods traffickers use to recruit and control their victims. This data can then be

analyzed using data science techniques to identify patterns and trends, such as the most common locations or methods used by traffickers.

2. Social Media Analysis: Social media platforms can also be a valuable source of data to identify human trafficking. Data science techniques can be used to analyze social media data to identify patterns of behavior that may indicate human trafficking. For example, social media posts that advertise job opportunities with vague descriptions or promise high-paying jobs with little or no experience can be used to recruit trafficking victims.

3. Language Processing (NLP): is a branch of data science that focuses on the interaction between computers and human language and can be used to analyze textual data, such as social media posts or online ads, to identify language patterns that may indicate trafficking. . For example, NLP techniques can be used to identify common phrases or words that traffickers use to recruit victims.

4. Machine Learning: is a branch of data science that involves using algorithms to learn patterns from data. It can be used to identify patterns of behavior that may be indicative of trafficking. For example, machine learning algorithms can be trained to identify common behavior patterns among trafficking victims, such as changes in location or behavior.

5. Data Visualization: Data visualization is the process of representing data in a visual format, such as graphs or charts. It can be used to help law enforcement agencies and other organizations better understand patterns and trends in human trafficking data. For example, data visualization can be used to create maps showing locations where human trafficking is most common or charts showing the types of trafficking that are most prevalent.

7. Challenges Facing Data Science in Combating Human Trafficking

While data science can be a powerful tool in combating human trafficking, there are several challenges that may arise during the analysis process. The main challenges include:

- Lack of standardized data: Often, data related to trafficking is incomplete or inconsistent, making it difficult to draw accurate conclusions from the available information.
- Ethical concerns: There are ethical considerations surrounding the use of data in trafficking investigations. Data on trafficking victims and traffickers must be handled carefully to protect the privacy and safety of those involved. Additionally, data analysis must be conducted in an unbiased manner to avoid false accusations and protect the rights of individuals who may be wrongly accused.
- Resource limitations: Data science can be limited by the resources available for data collection and analysis. Limited funding or staffing can make it challenging to collect and analyse large amounts of data, potentially reducing the effectiveness of data science in identifying and combating human trafficking.

Despite these challenges, data science has the potential to be a valuable tool in the fight against human trafficking. By leveraging data science techniques, law enforcement agencies and other organizations can better understand trafficking patterns and characteristics, which can aid in identifying victims and apprehending traffickers. As research and development continue, data science may become an increasingly important tool in the global effort to combat human trafficking (How Data Science Can Help Combat Human Trafficking: Techniques and Challenges | by Data Overload | Medium, 2023).

People may tend to think of law enforcement organizations and helpers rather than data scientists in the fight against human trafficking. However, big data analysis and the blindness of data scientists can play a significant role in stopping human trafficking. The ability of big data and data scientists to collect and analyse massive amounts of data and discover patterns within that data creates a number of opportunities to find victims and traffickers. Here are 5 ways data scientists are fighting human trafficking:

1. Identifying At-Risk People: There are many factors that increase the likelihood of a person being at risk of trafficking, such as unemployment, poverty, and fleeing a war-torn area. Data scientists can help combat trafficking by identifying these populations and the locations where individuals might be vulnerable to false job or romantic offers. Organizations can then direct resources to these areas.
2. Locating Victims: Big data can be used to identify when victims come into contact with medical professionals or law enforcement in scenarios indicative of trafficking. Certain patterns of charges at hotels may also signal trafficking activity, potentially helping locate the traffickers themselves.
3. Locating Traffickers: There are additional ways to use data to locate traffickers online. Surprisingly, traffickers sometimes hide in plain sight, using social media or dating sites. Some individuals frequently change their identities, but data analytics can use facial recognition and other techniques to identify them. Just as analytics can identify at-risk populations, it can also pinpoint events where traffickers might be active, allowing law enforcement to be alerted and structures to be put in place to help victims.
4. Tracking Financial Information: IBM developed a secure data centre to help banks and other financial institutions identify money laundering and other transactions related to trafficking. Data scientists can use both AI and machine learning to combat human trafficking. The centre also aggregates vast amounts of news and other data to better understand how traffickers recruit and move their victims. AI then puts this information into a format usable by financial institutions, NGOs, and governments.
5. Disrupting Networks: Disrupting networks requires cooperation between law enforcement and governments. Unfortunately, in some countries, they are not always cooperative. However, data scientists can combat trafficking by using advanced data analytics and help dismantle these networks. Data analytics can be used in various ways to detect patterns indicating human trafficking, analysing users, interactions, and connections on social media to identify traffickers, victims, and clients (5 Ways Data Scientists Fight Human Trafficking - Data Science Degree Programs Guide, 2023).

Cybersecurity and Human Trafficking

Cybersecurity involves tactics, techniques, and procedures for a range of investigative tools and processes, including interviewing, interrogation, counter-surveillance, and surveillance detection. It appropriately balances the benefits of prosecution against intelligence gathering. Due to the importance of combating human trafficking, some institutions offer professional certifications in investigating this crime to enhance the training and professional level of investigators. One such certification is the Certified Human Trafficking Investigator (CHTI), awarded to those who demonstrate expertise and competence in managing human trafficking investigations, intelligence gathering, digital evidence collection, interviewing and interrogation, and developing reports and testimonies to validate findings. CHTI credentials are the first of their kind in the industry, taught by world-class professionals who will teach you everything you need to know to be highly effective in combating the global issue of human trafficking (Certified Human Trafficking Investigator (CHTI) from McAfee Institute | NICCS (cisa.gov).

The following are the roles specific to this type of professional certification. It includes Knowledge, Skills, and Abilities (KSAs), which a Certified Human Trafficking Investigator is expected to possess:

1. **Abilities**

- Ability to search and navigate the dark web using the TOR network to identify markets and forums.
- Ability to examine digital media on multiple operating system platforms.
- Determine whether a security incident indicates a law violation requiring specific legal action.
- Identify digital evidence for examination and analysis to avoid inadvertent alteration.
- Identify elements of crime proof.
- Identify and collect documentary or physical evidence, including digital media and records related to cyber breach incidents, investigations, and operations.

2. **Knowledge**

- Knowledge of computer network concepts, protocols, and network security methodologies.
- Knowledge of risk management processes (e.g., risk assessment and mitigation methods).
- Knowledge of laws, regulations, policies, and ethics related to cybersecurity and privacy.
- Knowledge of cybersecurity and privacy principles.
- Knowledge of cyber threats and vulnerabilities.
- Knowledge of specific operational impacts of cybersecurity lapses.
- Knowledge of intrusion detection methodologies and techniques to detect host and network intrusions.

- Knowledge of threats and vulnerabilities associated with system and application security (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL injection, race conditions, covert channel, return-oriented attacks, and malicious code).
- Knowledge of insider threat investigations and reporting, investigative tools, laws/regulations.
- Knowledge of adversarial tactics, techniques, and procedures.
- Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, network-connected devices, network-connected home controllers, printers, removable storage devices, telephones, photocopiers, fax machines, etc.).
- Knowledge of digital evidence seizure and preservation.
- Knowledge of legal governance related to admissibility (e.g., rules of evidence).
- Knowledge of the collection, packaging, transportation, and storage of electronic evidence while maintaining the chain of custody.
- Knowledge of static data types and collection.
- Knowledge of the social dynamics of computer attackers in a global context.
- Knowledge of electronic evidence law.
- Knowledge of legal rules of evidence and court procedures.
- Knowledge of covert communication techniques.
- Knowledge of crisis management protocols, processes, and techniques.
- Knowledge of physical and physiological behaviours that may indicate suspicious or abnormal activity.
- Knowledge of judicial processes including fact and evidence presentation.
- Knowledge of applicable legislation, laws, regulations, and policies governing cyber targeting and exploitation.
- Knowledge of application security risks (e.g., OWASP Top 10).

3. Skills

- Skill in maintaining the integrity of evidence following standard operating procedures or national standards.
- Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid data alteration, loss, or physical damage.
- Skill in using scientific rules and methods to solve problems.
- Skill in evaluating the credibility of a source and/or product.
- Skill in interviewing victims and witnesses and conducting interviews or interrogations of suspects.
- Developing a plan to investigate crimes or incidents or suspicious activities involving computers and the internet.
- Establishing relationships, where possible, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).
- Examining retrieved data for information relevant to the matter at hand.
- Integrating computer network attack analysis with criminal investigations, counterintelligence operations.

- Using specialized equipment and techniques to catalogue, document, and extract digital evidence, collect, package, and preserve it.
- Assessing victim or witness behaviour or suspect in relation to the investigation.
- Determining the extent of threats and recommending courses of action or countermeasures to mitigate risks.
- Providing criminal investigation support to trial attorneys during judicial processes.
- Analysing computer threats for counterintelligence or criminal activity.
- Collecting and preserving evidence used in prosecuting computer crimes.
- Documenting the original state of digital evidence and/or associated evidence (e.g., through digital images, written reports, hash function examinations).
- Employing IT systems and digital storage media to solve cybercrimes and fraud committed against individuals and property, investigating and/or prosecuting perpetrators.
- Preparing reports to document the investigation according to legal standards and requirements (Cyber Investigation | NICCS (cisa.gov).

In an initiative that has gained significant traction, two individuals launched the "Hacking to Fight Trafficking" initiative, a non-profit organization founded by two executive MBA graduates aiming to foster innovation and combat human trafficking through hackathons and other platforms (Dhyani, 2023).

Human Trafficking Kill Chain

The ability to use technology for good has made promising strides in identifying and disrupting online human trafficking, and the human trafficking kill chain, as developed by the Global Liberation Network, offers a comprehensive approach to tackling this issue. The kill chain model provides a linear cognitive framework for addressing a complex, multifaceted crime, useful for making effective decisions in adversarial environments. The rigorous analytical framework enables stakeholders involved in anti-trafficking efforts, from law enforcement to businesses, to apply this approach. The terms detect, deny, disrupt, degrade, deceive, and destroy are used to distinguish between possible actions to weaken or destroy the adversary's ability to operate. It is important to note that these actions are arranged by the strength of the action and the amount of time the action impacts the adversary.

Brief Description and Course of Action for Each:

- Detect: The detection or identification of the presence or presence of something. In tactical operations, detection is the perception of an object of potential military importance that has not been confirmed. In the context of online human trafficking, detection is the preliminary identification of the presence of an online trafficking organization.
- Deny: In military terms, deny refers to depriving the enemy of the use of a thing. For anti-human trafficking efforts, this can mean restricting the trafficker's use of financial services, legitimate employment, websites, and access to new victims.

- Disrupt: Disruption is the ability to break up, interrupt, or prevent something from occurring. In an anti-trafficking context, it could involve actions such as seizing trafficker's bank accounts, detaining or arresting traffickers, or preventing the exploitation of specific victims.
- Degrade: Degradation is the ability to reduce the effectiveness or capability of an adversary to function, often through physical or psychological means. For online human trafficking, this could mean decreasing the trafficker's ability to recruit new victims, operate a trafficking website, or conduct financial transactions.
- Deceive: Deception involves misleading an adversary into making an incorrect decision or taking an inappropriate action. This could involve false postings or advertisements to lure traffickers into revealing themselves or providing misleading information to confuse the traffickers.
- Destroy: The ultimate goal in combating human trafficking is to destroy the ability of traffickers to operate. This involves the complete eradication of trafficking operations and the prosecution of the traffickers involved.

The value of applying the Kill Chain approach to human trafficking lies in automating as much of the process as possible to reduce the time needed to achieve value. It also highlights potential disruption strategies and combinations of actions to achieve the most substantial and longest-lasting impact. Disruption options also vary according to stakeholders.

However, by using cybersecurity techniques, including Kill Chain analysis, machine learning, network interception and visualization, consequence-based analysis, threat modeling and detection, and defense-in-depth, online content providers can disrupt human trafficking. We have successfully mitigated potential trafficking content and protected worker health. The following study discusses how to effectively utilize cybersecurity techniques on a large scale. (Borrelli & Caltagirone, 2021).

"KILL CHAIN ANALYSIS IS A GUIDE FOR ANALYSTS TO UNDERSTAND WHAT INFORMATION IS, AND MAY BE, AVAILABLE FOR DEFENSIVE COURSES OF ACTION." - LOCKHEED MARTIN

Kill Chain analysis serves as a guide for analysts to understand the information that is available and may be available for defensive actions.

It represents a new way of thinking about human trafficking, providing an informal tool to discover trafficker behaviours, predict future events, maximize intelligence opportunities, and track traffickers and victims over time and geography. This model also lays the foundation for a mathematical framework where theories and models of adversarial decision-making can be applied formally, allowing for testable hypotheses and effectiveness metrics.

8. Previous Work

In 2007, the U.S. Department of Defence described the process by which the military seeks to overcome its adversaries. The military Kill Chain includes the steps of reconnaissance, arming, delivery, exploitation, command and control (C2), and actions on the objective. The model is used to analyse, uncover, and consolidate operations on

the battlefield and to make quick yet rational decisions. Similarly, Lockheed Martin confirmed the existence of the Cyber Kill Chain in its foundational piece titled "Intelligence-Driven Computer Network Defence" which extends the battlefield model to the cyber world and applies it to advanced persistent threats. The following diagram illustrates how Lockheed Martin assesses each phase of the process, from reconnaissance to actions on the objective, for options to detect, deny, disrupt, degrade, deceive, or destroy adversary capabilities and assets.

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Cyber Kill Chain

Seo-Young Cho used Extreme Bound Analysis (EBA) to account for push and pull factors in human trafficking in destination and origin countries in "Modeling Determinants of Human Trafficking: An Empirical Analysis." He found it challenging to identify strong, reliable, and empirical data variables. This study statistically supports and refutes many of the underlying causes of human trafficking mentioned above. However, this represents the first and only attempt to create a statistical model and predict the factors of human trafficking. (Cho, 2015).

Human Trafficking Kill Chain

The human trafficking kill chain, as depicted below, organizes a complex and multi-dimensional crime into a linear cognitive model. Breaking down the human trafficking kill chain into its component parts enables stakeholders in anti-trafficking efforts to better confront their adversaries with equal or greater resources and strategy. It allows analysts and stakeholders to fully leverage current and future information to enhance their defensive and offensive options. The human trafficking kill chain consists of six

main elements: recruitment, transportation, entrapment, brokering, delivery, and exploitation.

We can detail each component to better understand its application and inclusion.

1. Recruitment: Recruitment is a crucial element of human trafficking and a key pillar of its legal definition. While this phase often involves personal communication or online activities such as ads and social media conversations, recruitment can also broadly describe targeting an individual to be trafficked. For the purposes of the trafficking kill chain, kidnapping is considered recruitment. News articles, interviews with survivors, traffickers, and case precedents highlight multiple recruitment methods. Some of these include:

- Social media platforms like Facebook, Twitter, and Snapchat.
- Job ads, such as modelling or agricultural labour opportunities.

2. Transportation: Transportation is another key pillar in the legal definition of trafficking, involving the movement and housing of victims. While there are cases where victims are not removed from their home environments, such as in online webcam sexual exploitation, victims are typically transported either willingly or by force. Some transportation methods include:

- Commercial or private planes.

3. Entrapment: Entrapment is one of the most critical aspects of the trafficking kill chain and perhaps the hardest to disrupt. Surprisingly, few human trafficking survivors consider themselves victims, often rejecting help or escape opportunities. Entrapment is as much psychological as it is physical. Some methods include:

- Locked rooms or buildings.
- Drug addiction.
- Confiscation of travel and identification documents.
- Remote locations.

4. Brokering: Brokering is the process of connecting the victim with the buyer. In some cases, the victim may self-broker, as in a child forced to hold a sign and beg at a public intersection. Brokering can take the following forms:

- Ads placed on public forums or online.
- Flyers, websites.
- Personal connections with potential buyers.

5. Delivery: This is when victims are transported from their holding place to the location of exploitation. In some cases, the exploitation occurs within the holding site. The methods used for delivery are often the same as those mentioned above for transportation. However, delivery can be remote, especially in the case of online exploitation. Additional delivery methods may include:

- Password-protected websites.
- Sending content via app, email, or URL.

6. Exploitation: Exploitation is the actual exchange of money or other benefits between the broker and the buyer, where the victim is required to do or be something that benefits the buyer. Examples of exploitation include:

- Sexual acts, including pornography and remote webcam work.
- Forced labour of all kinds.
- Prison labour (in some cases).

Understanding the duration and stages of the process allows for documenting and considering anti-trafficking operations in a formal analytical manner. Additionally, consider the assets that traffickers may use at each stage of the kill chain. Assets are what traffickers use at each stage of the kill chain to achieve their ultimate goal: money or other benefits, such as computers, mobile phones, internet connections, social media apps, videos, websites, etc. Below is a human trafficking kill chain analysis grid that is used to analyse human trafficking events and consider potential disruption opportunities. (Polaris Project, 2017).

Human trafficking kill chain matr

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recruitment						
Transportation						
Entrapment						
Brokering						
Delivery						
Exploitation						

As an example of a practical application of this chain, we begin with the known assets that traffickers have used and the situations they have exploited during each stage of the trafficking kill chain:

Case Study 1: Sex Trafficking in the United Kingdom

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recruitment	Collect prostitution advertisements in origin countries		Shut down prostitution advertisement websites		Place several false ads to make discovery difficult for traffickers	
Transportation	Pass airfare purchases through known trafficker CC database	Block purchases of airfare by known CC numbers				
Entrapment	Reporting of large numbers of cash-only transactions at banks					
Brokering	Collect prostitution advertisements in destination countries		.Shut down prostitution advertisement websites. .Purchase ban on burner cell phones			
Delivery	Pass transport purchases through known trafficker CC database					

Exploitation	. Pass hotel bookings through known trafficker CC database. . Report multiple cash hotel bookings to counter trafficking body					Lengthy sentences for traffickers

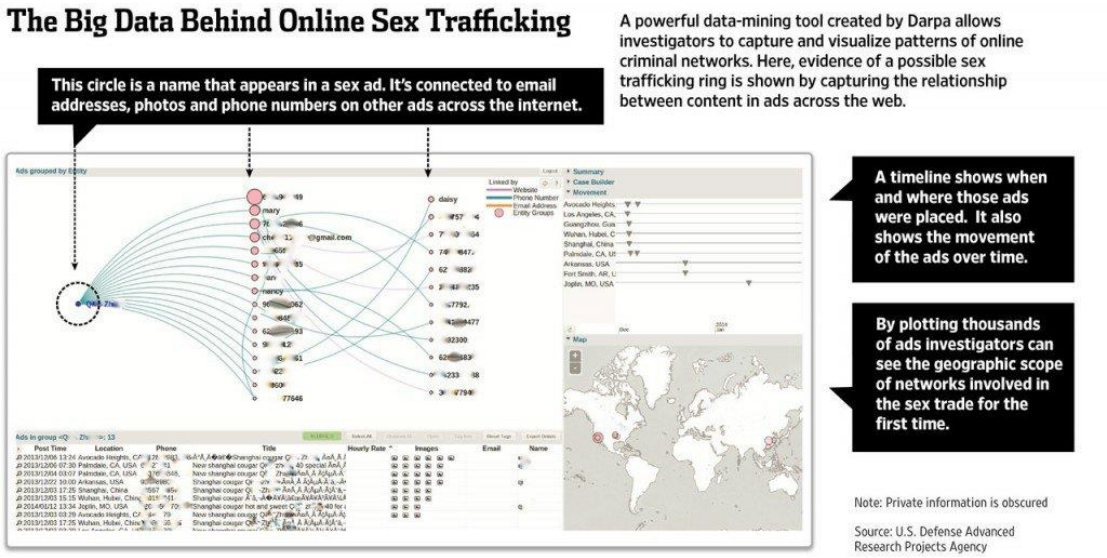
Use of Technology in Human Trafficking Investigations

Useful sources and evidence for digital evidence collection include:

- Phone data: Modern traffickers' and smugglers' reliance on their smartphones means there is a wealth of evidence available on these devices if accessed;
- Social media posts: Photos, videos, contacts, partners, locations, and other information can be gathered from social media accounts;
- Digital fingerprints, including browser history on personal computers and IP addresses.

A major obstacle to investigations is the time required to conduct them and the inability to engage in criminal activities, except for authorized "undercover" operations. Technology can be leveraged to reduce the time taken to identify perpetrators and victims and proactively remove content related to human trafficking/smuggling.

Another method to overcome investigative obstacles is to use web crawlers and data mining tools. DARPA's Memex program has developed tools to identify human traffickers and trafficking victims. As part of Memex, web crawlers and data mining tools have been developed that extract data from online advertisements (on the visible and deep web) and create databases using this information. These tools (such as DIG and Tell Finder) specifically comb through ads, download content, and identify links between downloaded items. The information in these databases is mined to identify trends, patterns, and visual maps. This mapping allows for identifying timelines and victim movements (See figure below).



DeepDive Applications - DeepDive (stanford.edu)

9. Results and Recommendations

To minimize the abuse of technology to facilitate human trafficking and maximize the value of technology-based solutions for this crime while ensuring that ethical considerations are fully addressed, the following recommendations are made for all actors involved in using technology to combat trafficking:

- Expand partnerships and alliances among different sectors and stakeholders, including international and regional organizations, the public sector, survivors, civil society, the private sector, and academia, to promote research, innovation, development, and use of technology.

- Identify and address legal system gaps to ensure effective investigation and prosecution of technology-enabled trafficking, including coordinating laws and enhancing cross-border cooperation to combat the transnational threats posed by technology-enabled trafficking.

- Significantly expand data collection and research on the scope, scale, and nature of technology abuse to facilitate human trafficking, particularly online.

- Build expertise and capacity among practitioners across sectors to maximize the use of technology to combat human trafficking.

- Support law enforcement in establishing a presence in the online world, conducting proactive operations, seizing appropriate evidence, and using available technology tools to combat human trafficking.

- Increase support for technology-based solutions to identify trafficking victims and cases.

- Support technology-based policies and solutions that address the global scope of human trafficking, such as scalable online prevention programs or data aggregation tools that facilitate large-scale analysis to support human trafficking investigations.
- Ensure that new anti-trafficking initiatives do not duplicate existing technology-related efforts.
- Explore political and operational solutions to address the misuse of technology platforms, including websites that may be used to facilitate human trafficking.
- Incorporate a gender-sensitive perspective when addressing the relationship between trafficking and technology, including addressing the continuing violence against women and girls that occurs online, such as sexual extortion, harassment, and sham marriage ads, as a means of gender-based coercion and control that perpetuates trafficking in women and girls. The benefits provided by advanced technology should consider gender differences, including by facilitating easy reporting and ensuring that victims quickly and effectively receive help if targeted by repeated abusive behaviour online, putting them at greater risk of trafficking and exploitation (ICAT 2019).

Future Work

Additional work is needed in the areas of image and video analysis, especially regarding text extraction, emoji's, filters, and Unicode from images and real-time processing of live video feeds. Further research is also important on de-anonymizing cryptocurrencies. Most importantly, tools need to be developed to collect, analyse, and distribute information derived from the human trafficking kill chain to all relevant stakeholders. The more we safely share relevant information with necessary partners, the greater our impact on the global crime of human trafficking.

Conclusion

When a trafficker starts using the Internet or cyberspace as a tool, trafficking can be considered a cybercrime and falls within the scope of legal texts dealing with cybercrimes. Web browsing and protecting users from involvement either as potential victims or as customers using the Internet are essential for effective prevention efforts. It must be understood that human trafficking is not just a problem for states but concerns communities and citizens worldwide. This phenomenon can only be prevented through collective confrontation of the issue. For this reason, raising awareness in the media and civil society is an important tool for preventing Internet-related trafficking. Cooperation can also be an effective tool by governmental organizations and the private sector to protect vulnerable people; to prevent re-trafficking and re-victimization. The challenge we face today is that we must respond to global crime with global legislation, or all attempts will remain fragmented, and we will be unable to escape this cycle of violations and trafficking crimes.

10. References

[1]. Europol. (2016). Situation report: Trafficking in human beings in the EU. Europol Public Information, 765175
[2]. Emerging Global Threats Related to Online Child Sexual Exploitation (OCSE) – ECPAT, 2017.
[3]. A list of technology tools developed to support efforts to combat human trafficking can be found here: https://www.bsr.org/files/ BSR_list_of_technology_tools_identified_by_tech_against_trafficking, 2019.
[4]. human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf, 2019.
[5]. Brieanna Charlebois. Cyber trafficking. Available at URL: https://www.blueline.ca/cyber-trafficking/ September 30, 2021.
[6]. Julie Jones is the founder and CEO of Human-i Intelligence Services, an exclusive cybersecurity, investigations, and threat management company based in Vancouver, Canada.
[7]. United Nations Office on Drugs and Crime, Case Law Database, SHERLOC, 2007, case no: BRA004. URL: https://sherloc.unodc.org/cld//case-law-doc/criminalgroupcrimetype/bra/2007/processo_n_2004.81.00.18889-0.html?lng=en&tmpl=sherloc
[8]. United Nations Office on Drugs and Crime, Case Law Database, SHERLOC, 2011, Case no. SWE014. Also available at URL: https://sherloc.unodc.org/cld//case-law-doc/traffickingpersonscrimetype/swe/2011/case_no_b_87-11.html?lng=en&tmpl=sherloc
[9]. Lusthaus, J. & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. Policing: A Journal of Policy and Practice: https://doi. org/10.1093/police/pax042.
[10]. United Nations Children's Fund (UNICEF), The State of the World's Children: Children in a Digital World, 2017. URL: https://www.unicef.org/reports/state-worlds-children-2017.
[11]. United Nations Office on Drugs and Crime, Case Law Database, SHERLOC, 2014, case no. BEL034. URL: https://sherloc.unodc.org/cld//case-law-doc/traffickingpersonscrimetype/bel/2014/case_n_210814.html?lng=en&tmpl=sherloc
[12]. United Nations Office on Drugs and Crime, Case Law Database, SHERLOC, 2016, case no. SGP003. URL: https://sherloc.unodc.org/cld//case-law-doc/traffickingpersonscrimetype/sgp/2016/pp_v_muhammad_khairulanwar_bin_rohmat.html?lng=en&tmpl=sherloc
[13]. Vosler, Chase A. 2020. "Identifying Sex Trafficking in a Digital Environment Through Open-Source Intelligence." Master's Thesis, Department of Cybersecurity, Old Dominion University.
[14]. Barney, David. 2018. "Trafficking Technology: A Look at Different Approaches to Ending Technology-Facilitated Human Trafficking." Pepperdine Law Review 45:747-784.
[15]. Dukes, B. (2020). The Cyberworld and Human Trafficking: A Double-Edged Sword. ODU Digital Commons - Cybersecurity Undergraduate Research Showcase: The Cyberworld and Human Trafficking: A Double-Edged Sword.
[16]. Cyber Scamming as a New Destination for Human Trafficking Victims (csis.org), August 17. 2023
[17]. Victoria Garcia, 'Cybersex Trafficking: Grooming & Exploitation Online', (The Exodus Road, 15 March 2019), available at: Cybersex Trafficking: Grooming and Online Exploitation - The Exodus Road.
[18]. Joshua T. Carback "Cybersex Trafficking: Toward a More Effective Prosecutorial Response", (2018), Criminal Law Bulletin, 54 (1): 64–183; "International Efforts by Police Leadership to Combat Human Trafficking". FBI Law Enforcement Bulletin. 8 June 2016.
[19]. Cyber-trafficking, Available at URL: Cyber-trafficking | Law and Internet Foundation (netlaw.bg), 20.05.2022.

[20]. How Data Science Can Help Combat Human Trafficking: Techniques and Challenges. Available at URL: https://medium.com/@data-overload/how-data-science-can-help-combat-human-trafficking-techniques-and-challenges-969b29c4a135, 2023.
[21]. 5 Ways Data Scientists Fight Human Trafficking, Available at URL: https://www.datasciencedegreeprograms.net/lists/5-ways-data-scientists-fight-human-trafficking/, 2023.
[22]. "Thailand Toughens Rape Laws". VOA News. Available at URL: Thailand Toughens Rape Laws (voanews.com), June 1, 2019.
[23]. "Nepal Failing to Protect Women from Online Abuse". Human Rights Watch. Available at URL: Nepal Failing to Protect Women from Online Abuse | Human Rights Watch (hrw.org), May 18, 2020.
[24]. Borrelli, D., & Caltagirone, S. (2020). Non-traditional cyber adversaries: Combatting human trafficking through data science. Cyber Security: A Peer-Reviewed Journal, 4(1), 77-90.
[25]. Anuj Dhyani, Intern, CyberPeace Foundation Cyber Enabled Human Trafficking – An Overview, Available at URL: Cyber Enabled Human Trafficking – An Overview – CyberPeace Corps, 2023.
[26]. Hacking to fight trafficking. Available at URL: Hacking to fight trafficking | MIT News | Massachusetts Institute of Technology, 2018.
[27]. Cyber Investigation, Available at URL: https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-investigation.
[28]. Certified Human Trafficking Investigator (CHTI), McAfee Institute, 7950 NW 53rd St, STE 337, Miami, FL 33166, available at URL: https://niccs.cisa.gov/education-training/catalog/mcafee-institute/certified-human-trafficking-investigator-chti.
[29]. Trafficking in Persons & Smuggling of Migrants Module 14 Key Issues: Technology Facilitating Trafficking in Persons (unodc.org), 2021.
[30]. Polaris Project. (2017). The Typology of Modern Slavery. Washington, DC: polarisproject.org. Retrieved from http://polarisproject.org/sites/default/files/Polaris-Typology-of-Modern-Slavery.pdf
[31]. Cho, S. Y. (2015). Modeling for determinants of human trafficking: An empirical analysis. Social Inclusion, 3 (1), 2–21.
[32]. Caltagirone, S. (2017). The human trafficking kill chain: A guide to systematic disruption.