Modern Slavery

Issue Brief

JANUARY 2022

Digital Intelligence: New opportunities to be harnessed in the fight against human trafficking

The digital revolution of the last decade has led to the emergence of new, computer-related modalities of human trafficking and sexual exploitation crimes. By increasing perpetrators' and consumers' anonymity, providing access to safe encrypted technologies and reaching wider audiences, new digital technologies have become instrumental in advertisement, recruitment, and the exploitation of victims without the need for face-to-face encounters or geographical proximity, and with relatively little investment on the part of perpetrators.[1] The COVID-19 pandemic has created additional opportunities for traffickers – with higher levels of vulnerability due to the deteriorating economic environment and increased online activity.

Despite these trends, the digital revolution has opened several opportunities to more effectively, and efficiently, combat human trafficking. The prevalence of digital devices in our everyday lives and the centrality of the internet in human communications means that there are vast quantities of "digital evidence" available to law enforcement agents, prosecutors and judges that can be used to combat trafficking. The digital trail left by perpetrators and victims of human trafficking can be harnessed through "digital forensics", "a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on data stored on a computer, digital device or other storage media".[2]

The evidence gathered through digital forensics can be aggregated, synthetised and summarised in order to identify offenders, prevent future crimes, reduce investigative times and expedite prosecution and judicial procedures. Digital evidence can also help law enforcement corroborate victim statements, mitigating the risk of re-traumatisation and strengthening cases,

Key Findings and Recommendations

- Rapid technological advances have provided traffickers with an unprecedented ability to securely advertise, recruit and exploit victims at scale. The COVID-19 pandemic has only exacerbated this trend.
- The digital trail left by these activities creates new opportunities to identify offenders, prevent crimes, reduce investigation times, and expedite prosecution and judicial procedures.
- Unlocking this potential relies on law enforcement and criminal justice systems overcoming key technological, legal and resource challenges.
- Promising practices are emerging - particularly in the area of financial intelligence alliances, and the development of digital tools by NGOs and technology providers in support of law enforcement investigations.
- More needs to be done to increase law enforcement and judicial system capability in digital forensics, with clear guidance on admissible ways to obtain and use digital information.
- Greater collaboration between enforcement authorities, NGOs and private technology providers should be fostered if key constraints are to be overcome.
- Multinational instruments aimed at fostering international cooperation concerning electronic evidence and how it is used in criminal matters need to be developed.

particularly when victim testimony may be perceived as unreliable - underlining the need to update legal systems to allow the use of digital footprints in investigations and prosecutions.

Nonetheless, the possibility of taking advantage of these developments in digital forensics is critically dependent on the ability of law enforcement agencies and the criminal justice system to overcome key technological, legal and financial challenges posed by the digital revolution.

Technological challenges

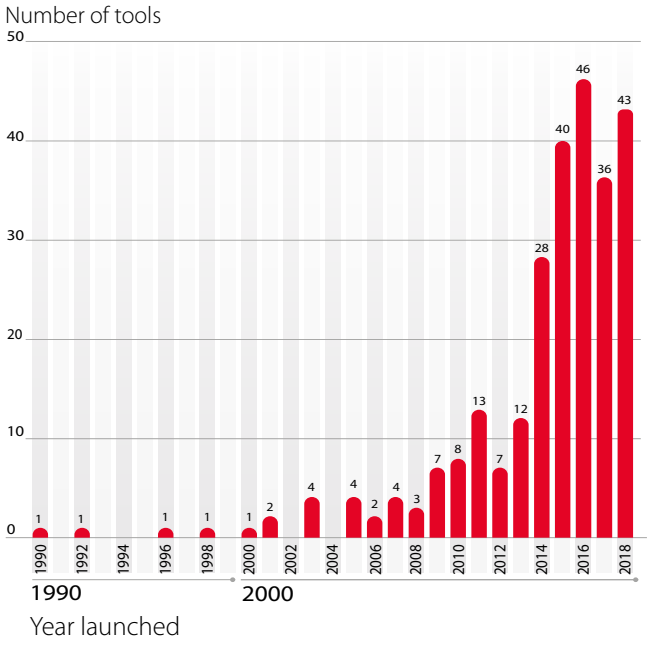
A key problem faced by law enforcement agencies working on digital intelligence is the sheer range of devices, operating systems, and data formats used by human traffickers, which pose considerable technical challenges for carrying out digital forensics. This proliferation of device types and data formats makes it hard to generate consistency in the outputs of digital forensic work.[3] This is further complicated by the lack of interoperability of IT systems between national and international law enforcement agencies, which makes it difficult to share and compare forensic outputs within and across borders.

Additionally, law enforcement agencies around the world typically use poor or outdated technologies, while criminal networks have access to more sophisticated technologies. Although law enforcement agencies have become increasingly more skilled in the use of digital technology over the past decade, they still lag behind criminal groups. Moreover, given the fast pace at which new digital technologies evolve, the lag between the technology used by law enforcement authorities and that used by human traffickers is likely to worsen even further.[4]

While these issues could in principle be addressed by establishing links and cooperation between public and private organisations, much of the literature underscores that such systematic collaborations are still quite limited.[5] Notable exceptions however can be found in the financial industry, where Financial Intelligence Units (FIUs), major banks, remittance service providers, and law enforcement agencies have come together in a number of jurisdictions to share intelligence and skills and deliver innovative solutions to detect, disrupt and prevent human trafficking.

Recent years have seen a surge in the development of technological tools for combatting human trafficking (see Figure 1). A number of technology providers and NGOs are actively supporting law enforcement efforts through the development of specialist technology and analytical tools that help better identify exploitation, and turn large volumes of data into actionable intelligence.[6]

Technology tools combatting Human Trafficking launched.



Source: OSCE (2020). Leveraging Innovation to Fight Trafficking in Human Beings: A comprehensive analysis of Technology Tools.

Legal challenges

The lack of case law, and the uncertainties around the scope of proof and requisite evidentiary needs that flow from this are key challenges to the use of digital evidence in the fight against human trafficking. Additionally, issues around the ability of legal authorities to access data, the admissibility of electronic evidence and uncertainties around the chain of custody of evidence, cross-border searches and seizures, are all difficulties that the national justice systems of most countries face when dealing with digital evidence.[7] Privacy and ethical concerns around the possibility of using digital evidence without undermining the fundamental right of both victims and other individuals who may be collaterally affected must also be considered.[8]

Legal aspects also hamper international collaborations that would allow the exchange of technology. A key problem is the different approach that national states take to regulating the cyberspace. While countries like

China, Russia and many developing nations adopt a state-led approach based on territorial and national-sovereignty concerns, advanced democracies like the US, the UK and most European countries prefer a multi-stakeholder model that includes private-sector (most notably, technology developing) actors. This difference carries implications for the treatment of data regulation and privacy as well as for trans-border access to digital evidence - which is critical to boost the efficacy of cybercrime investigations.[9]

Finally, in the case of financial investigations associated with human trafficking, a specific legal issue faced by FIUs is that human trafficking activities are often embedded in legal business and the legal economy, which makes the legal aspects of digital forensics applied to financial transactions particularly complex.[10]

Resource Challenges

While the demand for digital forensics – and the available digital evidence – has grown exponentially over the last few years, human resources appropriately trained in digital forensics are scarce in most law enforcement agencies. A stylised finding emerging from a broad review of comparative and international literature is that the digital knowledge of frontline officers involved in human trafficking cases is often out of date and needs to be improved.

In the UK, the amount of money spent by police forces on forensics has halved over the last decade, despite this exponential growth in demand. Additionally, police enforcement agencies in the UK are experiencing a "brain drain" of digital experts moving to the private sector, where individuals with this type of skills can typically earn higher salaries. According to the UK Police Foundation, staff numbers trained in digital forensics would need to grow by between a third and 50% in order to meet the demand.[11]

In the case of the financial industry, it is important to note that, in addition to the shortage of expertise and skills, relatively low political weight is placed on financial investigations. This is driven by the relatively "small" financial "rewards" associated with financial investigations of human trafficking cases compared with the proceeds from other types of crime (drug trafficking, VAT fraud, theft). The fragmented nature of the human trafficking business and the relatively small size of most criminal networks further exacerbates this problem.[12]

Promising practices

In the last few years, a growing number of NGOs have supported law enforcement agencies faced with limited human and technological resources. For instance, Thorn, an NGO that uses tech-led approaches to combat online child sexual abuse, developed a tool to aggregate data from online commercial advertisements. This tool is now used by police authorities in the US, and Canada to identify victims of exploitation and is credited with a 60% reduction in investigation time. In Thailand, Justice and Care partner, LIFT International, has a small team of researchers devoted to digital forensics work. This team combines the monitoring of open-source information with more sophisticated extraction techniques and analyses in support of the country's law enforcement and justice system. LIFT's work has contributed to the arrest of 63 human trafficking offenders and 34 convictions in 2020 alone.

Resources to fight human trafficking are, in fact, becoming increasingly available. Tech Against Trafficking, a coalition of technology companies working to combat human trafficking supported by international organizations such as the Organisation for Security and Co-operation in Europe (OSCE) and the International Organisation for Migration (IOM), has mapped more than 260 technological tools that can be used to support anti-trafficking work. These include web-scraping software that can be used to extract online job advertisements and gather information from commercial sex websites, blockchain technologies which allow tracking the production of goods from their source to their final destination to increase transparency in supply chains, and satellite imagery and geospatial mapping tools used to identify and locate remote and high-risk populations that may be vulnerable to trafficking.[13]

Further cause for optimism comes from a number of alliances - such as the Fintel Alliance and Banks Alliance against Trafficking[14] - which have been established to help the financial sector detect and combat criminal exploitation, and support law enforcement in their investigations. These multi-stakeholder groups bring together experts from a range of organisations including financial institutions, remittance service providers, NGOs and law enforcement authorities.

Significant progress has especially been made in the area of Online Sexual Exploitation of Children. FINTRAC

(the Canadian FIU), AUSTRAC (the Australian FIU), Philippine Anti-Money Laundering Council and OSEC's Information Exchange Working Group have compiled lists of keywords and financial transaction patterns related to OSEC activity, informing Suspicious Activity Reports issued by financial institutions. In 2020 alone, Philippine law enforcement identified 147 suspects in the Philippines for joint investigations of child sex trafficking and money laundering based on an analysis of suspicious money transfers associated with these indicators.

Payments for other types of Modern Slavery have, however, been harder to detect. Reporting entities have struggled to identify cases involving labour exploitation, for example, because of the difficulty of identifying and isolating proceeds from labour exploitation mixed with legitimate business revenue. Analysis to date has also primarily focused on transactions intersecting with financial institutions primarily in developed countries, with less attention on transactions related to bonded labour in South Asia or migrant workers in the Gulf. New risk-analysis tools and methods may be needed to better understand how modern slavery and human trafficking intersects with the remittance sector, money services businesses, and microcredit organizations in those contexts.[15]

Moving Forward

If digital intelligence is to be truly harnessed in the fight against human trafficking - improving detection, saving investigation time and strengthening prosecution cases - then significant challenges need to be overcome. Promising practices are emerging but more needs to be done to increase law enforcement and judicial system capabilities, and to foster greater collaboration with NGOs and private technology providers, and better international cooperation regarding sharing and using digital evidence.

[1] Europol (2021). The Challenges of countering human trafficking in the digital era.

[2] Interpol (2019). Global Guidelines for Digital Forensics Laboratories.

[3] Lillis, Davis, et al. (2016). "Current challenges and future research areas in digital forensic investigation". In: The 11th ADFSL Conference on Digital Forensics, Security and Law, Daytona Beach, Florida, May 2016.

[4] Muir, Rick, and Walcott, Stephen. (2021). Unleashing the Value of Digital Forensics. The Police Foundation.

[5] United Nations Office on Drugs and Crime - UNODOC (2013). Comprehensive Study on Cybercrime.

[6] OSCE (2020). Leveraging Innovation to Fight Trafficking in Human Beings: A comprehensive analysis of Technology Tools.

[7] Greiman, Virginia, and Christina Bain (2019). "The emergence of cyber activity as a gate to human trafficking". International Journal of Warfare and Terrorism 12(2): 41-49.

[8] Gerry, Felicity, Muraszkiewicz, Julia and Vavoula, Niovi (2015). "The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns". Computer Law & Security Review 32(2): 205-217.

[9] Walker, Summer (2019). Cyber-Insecurities: A guide to the UN cybercrime debate.

[10] Middleton, Ben, Antonoupoulos, Georgios, and Papanicolau, Georgios (2019). "The financial investigation of human trafficking in the UK: legal and practical perspectives". Journal of Criminal Law 83(4), 284-293.

[11] Muir and Stephen (2021).

[12] Middleton (2019).

[13] OSCE (2020).

[14] Thomson Reuters Foundation (2020). Banks Alliance Against Trafficking.

[15] United Nations University Centre for Policy Research (2019). Unlocking Potential: A Blueprint for Mobilizing Finance Against Slavery and Trafficking.

Digital Intelligence:
New opportunities to be harnessed in the fight against human trafficking
JANUARY 2022

Nicole Munns International Systemic Change Director
Gabriel Katz International Systemic Change Research Associate

Suite 139,
210 Upper Richmond Road,
London SW15 6NP

hello@justiceandcare.org
+44 (0)203 959 2580
www.justiceandcare.org