Cyber Security: A Peer-Reviewed Journal

This proof is sent to you by Kim Storry on behalf of Henry Stewart Publications. Please ensure you reply to kim@fakprepress.co.uk and copy in robert@hspublications.co.uk. Please check the proofs carefully.

It is preferable if you could annotate the pdf using comment boxes, please clearly give any answers to queries and/or corrections. We can also accept marked corrections and answers to queries from a scanned pdf, however if using this method please ensure any marking is clearly legible. Alternatively, if corrections are light, we can accept these supplied either in a word file or directly in an email, but please indicate the page number, col and line number so that we can identify where corrections need to be made.

Important: Please return your signed copyright form and marked proof with answered queries within 5 working days to kim@fakprepress.co.uk and copy in robert@hspublications.co.uk.
Authors are strongly advised to read these proofs thoroughly because any errors missed may appear in the final published paper. Once published, no further changes can be made.

If you have **no corrections** to make, please email confirming your approval to publish to kim@fakprepress.co.uk and robert@hspublications.co.uk.

The proof is sent to you for correction of typographical errors only. Revision of the substance of the text is not permitted, unless discussed with the editor of the journal. Only **one** set of corrections are permitted.
Please answer carefully any author queries.
Corrections which do NOT follow journal style will not be accepted.
A new copy of a figure must be provided if correction of anything other than a typographical error introduced by the typesetter is required. Colour images received will be set as colour figures throughout the proofing stages, but may not appear in colour in the final printed issue. However, full colour figures will appear in the online edition.
If you have problems with the file please contact kim@fakprepress.co.uk

Please note that this pdf is for proof checking purposes only. It should not be distributed to third parties and may not represent the final published version.

Kim Storry
kim@fakprepress.co.uk
on behalf of Robert Tamplin
Production Editor
Henry Stewart Publications
Ruskin House
40–41 Museum Street
London WC1A 1LT
Tel: +44 (0)20 7092 3481 (direct)
Fax: +44 (0)20 7404 2081
E-mail: robert@hspublications.co.uk

Non-traditional cyber adversaries: Combatting human trafficking through data science

Received (in revised form): 21st March, 2020

Danielle Borrelli

Operations Coordinator, California Cybersecurity Institute and Program Lead, Trafficking Investigations Hub, USA

Danielle Borrelli is the Operations Coordinator at the California Cybersecurity Institute (CCI) and the Program Lead for the Trafficking Investigations Hub (TIH). She oversees the implementation of all CCI events, training courses and projects, as well as develops and delivers training and technical resources that address the role of technology in recruiting and exploiting victims of human trafficking. In addition, Danielle is a local, regional and international anti-human trafficking advocate with nine years' experience in prevention, intervention and restoration work. Previously serving on the San Luis Obispo (SLO) County's District Attorney's Human Trafficking Task Force as their Housing Subcommittee Chair, Danielle has helped start and consulted on the development and sustainability of four separate housing programmes. Danielle also works with schools and businesses to provide training in human trafficking awareness. In addition, she provides mentoring to survivors of trafficking, and counselling to victims of sexual assault and domestic violence. Danielle was recently named California Polytechnic State University's Employee of the Year for 2018–19, SLO Tribune's Top 20 under 40 for 2019 and Jordan Cunningham's 35th District Woman of the Year.

California Cybersecurity Institute and Program Lead, Trafficking Investigations Hub, Building 631, 2303 Napa Ave,
San Luis Obispo, CA 93405, USA
Tel: 805-756-1341; E-mail: dborrell@calpoly.edu

Sherrie Caltagirone

Founder and Executive Director, Global Emancipation Network, USA

Sherrie Caltagirone is the founder and executive director of Global Emancipation Network (GEN), the leading data analytics and intelligence non-profit dedicated to countering human trafficking. Prior to starting GEN, Sherrie served as a policy adviser for Orphan Secure, a global human trafficking rescue non-profit, and began her anti-trafficking career with The Protection Project at the Johns Hopkins University. Sherrie served as a distinguished research scholar at North Carolina State University and is driven by research on the use of data analytics and mathematical models to combat trafficking, measuring criminal economies and polycriminality. She is the author of several international legal policies and guidelines on trafficking and has collaborated with the United Nations, League of Arab States, Council of Europe, Interpol and several governmental agencies to end modern-day slavery. Sherrie enjoys travelling and reads voraciously to feed a passion for creating new solutions to end human trafficking. She received her degree in international relations summa cum laude from American University.

Global Emancipation Network, USA
E-mail: sherrie@globalemancipation.ngo

Abstract Human trafficking is a complex and challenging global crime exacerbated by the use of technology. Traffickers utilise technology for scalability, anonymity and profitability as the Internet, social media platforms and encrypted messaging make the recruitment, exploitation and profit of an individual a low-risk, high-reward enterprise. Counter-trafficking efforts are often siloed approaches, resulting in decentralised information and analysis on the size and scope of trafficking in persons. Resources and tools such as the human trafficking kill chain methodology and Artemis, a machine learning (ML) human trafficking risk classifier, show promising disruption tactics which may also be applied to other asymmetrical threats. Recommendations for centralised data collections methods, interagency collaboration and cybersecurity adjacent legislation are also made.

KEYWORDS: trafficking, sexual, exploitation, cyber, adversaries, data

INTRODUCTION

Human trafficking is an international scourge affecting an estimated 40.3m individuals worldwide.[1] Victims endure physical, mental and sexual abuse, with 68 per cent of surveyed victims meeting the criteria for post-traumatic stress disorder.[2] Human trafficking is the second most profitable crime globally, a means to exploit vulnerable populations, advance compliance with terrorists through fear, sexual slavery and abuse, and thus threatens national, and indeed global, security.[3] It is an issue exacerbated by industrialisation and technological development, as traffickers utilise the scalability, efficiency and profitability provided by such advancements to exploit individuals. Services, tools and technology such as social media platforms, encrypted communications, online advertising sites, deep web sites and user-generated video sharing applications enable traffickers to hijack legitimate services for illicit purposes. Traffickers' very reliance on these tools, however, enables counter-trafficking stakeholders a window into effective means to combat them. While organisations across the globe have struggled to understand the size and scope of trafficking, new data collection, data science and artificial intelligence (AI) technologies and kill-chain methodologies show promising direction for disruption of human trafficking on a large scale. This paper dissects the intersection of technology and human trafficking, presents cyber strategies to combat these unconventional cyber adversaries and suggests recommendations for counter-trafficking stakeholders.

Human trafficking is defined by the United Nations 'Protocol to Prevent, Suppress, and Punish Trafficking in Persons, Supplementing the United Nations Convention Against Transnational Organized Crime' defines trafficking as:

> 'the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.'[4]

The global legislative framework also includes historical instruments dating back to the abolition of slavery:

- Slavery Convention, 1926;
- Supplementary Convention on the Abolition of Slavery, the Slave Trade, and the Institutions and Practices Similar to Slavery, 1956;
- Universal Declaration of Human Rights, 1948.

More modern legal instruments include regional and national approaches, including:

- Trafficking Victims Protection Act, US, 2000;
- Mekong Ministerial Initiative Against Trafficking (COMMIT), 2005;
- Council of Europe Convention on Action Against Trafficking in Human Beings, 2008;
- UK Modern Slavery Act, UK, 2015.

Unfortunately, however, these instruments have made significant gains in other areas, they have failed to address the issue discussed at length in this paper: the intersection of technology and human trafficking. The authors will discuss one law, FOSTA/SESTA, which attempted to hold online content providers accountable for trafficking on their services later in this paper.

INTERSECTION OF TECHNOLOGY AND HUMAN TRAFFICKING

As documented above, human trafficking was not defined as such internationally, much less across individual nations, prior to 2000. Data collection on the scope of the problem has thus been difficult. It can be argued the most reliable historical figures come from the 'United States Department of State Office to Monitor and Combat Trafficking in Persons annual Trafficking in Persons Report', (see Table 1).[5] Numbers in parentheses refer to labour trafficking victims identified, prosecutions and convictions.

While human trafficking case data are inherently flawed due to the difficulty of identifying victims, inconsistencies in training for counter-trafficking agencies, inter-governmental cooperation and disparate laws, policies, definitions and approaches for prosecuting traffickers, reports indicate human trafficking is increasing.[6] Accounting for these and other variables, it is abundantly clear that trafficking in persons is a global humanitarian crisis. Global surges in technological developments, most notably the widely available connection to the Internet, has arguably jettisoned human trafficking rates. According to Pew Research, in 1999 only 41 per cent of the US adult population utilised the Internet.[7] Today, there are 4.1bn Internet users worldwide,[8] with 294m users (roughly 7.1 per cent of total users) from the US.[9] Traffickers utilise technology for its effectiveness in targeting available, vulnerable and desirable potential victims, the anonymity the Internet provides and scalability it offers for profit and reach. Prior to the mass distribution and availability

Table 1: Historical figures from the United States Department of State Office to Monitor and Combat Trafficking in Persons Annual Trafficking in Persons Report

Year	Victim Identifications	Prosecutions	Convictions	New or Amended Legislation
2018	85,613 (11,009)	11,096 (457)	7,481 (259)	5
2017	96,960 (23,906)	17,471 (869)	7,135 (332)	5
2016	68,453 (17,465)	14,939 (1,038)	9,072 (717)	25
2015	77,823 (14,262)	19,127 (857)	6,615 (456)	30
2014	44,462 (11,438)	10,051 (418)	4,443 (216)	20
2013	44,758 (10,603)	9,460 (1,199)	5,776 (470)	58
2012	46,570 (17,368)	7,705 (1,153)	4,746 (518)	21
2011	42,291 (15,205)	7,909 (456)	3,969 (278)	15
2010	33,113	6,017 (607)	3,619 (237)	17
2009	49,105	5,606 (432)	4,166 (335)	33
2008	30,961	5,212 (312)	2,983 (104)	26
2007	–	5,682 (490)	3,427 (326)	28
2006	–	5,808	3,160	21
2005	–	6,618	4,766	41
2004	–	6,885	3,025	39
2003	–	7,992	2,815	24

of the Internet and subsequent social media platforms, trafficking in humans came with specific risks. As an example, before the massive rise of social media, trafficking victims forced into prostitution were forced to advertise their services on the streets. In doing so, an individual potentially had exposure to a dozen clients within a square mile. Within such a timeframe a victim is also exposed not only to the elements, affecting their health and longevity, but also to individuals looking to intervene (ie law enforcement). Consequently, inherent risk and potential loss of revenue was somewhat high for a trafficker. Mass Internet usage, however, makes the exploitation of sex trafficked individuals easier and more lucrative. Currently, online advertisements and review boards can reach up to thousands of potential clients from a much broader area. Online interactions between traffickers and potential victims and clients are often encrypted and anonymous, especially for those using apps such as WeChat, Vibe, Kik and WhatsApp, making it a preferred choice for both recruitment, entrapment and brokering. Some reports show that recorded content of any sexual exploitation can be and often is resold and or traded on abuse sites for additional revenue.[10] The very online nature of sexual abuse material makes interdiction and conviction difficult.[11]

> 'Online sexual exploitation often occurs across multiple jurisdictions, with victims and offenders often in different countries. Some countries are yet to update legislation that criminalizes the viewing or possession of child sexual abuse material online.'[12]

Often, manipulated content is used as further leverage to coerce production of more tradable and sellable abuse content or to force the victim to engage in physical interactions.[13] Sextortion, according to the National Center for Missing and Exploited Children (NCMEC), involves the same tactics of grooming, manipulation and coercion to obtain increasing amounts of explicit content.[14]

HARM OF TECHNOLOGY

Recruitment methods that used to be common within neighbourhoods, near schools and at transport hubs are now practised on social media platforms, gaming sites and other online forums. Vulnerability of an individual is still exploited, but new methods often rely on online personas and pretend admirers. Inherent trust of technology and simplified anonymisation makes recruitment almost seamless and predictable. Grooming — a term often used to describe the process whereby a perpetrator/predator identifies a vulnerable individual and begins to earn their trust through false claims of love, affection, provision and protection or anything that can be used as leverage against an individual — is maximisable through multiple anonymous accounts and thousands of targets from which to choose.[15] According NCMEC, online enticement and other forms of sexual abuse online has grown exponentially in the past 20 years. A minor issue in the 1990s is now an epidemic, with 10.2m reports of child abuse images in 2017.[16] Just recently, litigation towards Facebook and several other online content providers show the reality of human trafficking online.[17] Victims have argued that traffickers would not have the same access to them without leveraging such platforms.

Increased availability of technological resources leaves impoverished populations particularly at risk for trafficking. According to the International Justice Mission (IJM), cybersex trafficking is a new phenomenon affecting countries where fluency in English, Internet in almost every home and poverty are commonplace.[18] Such conditions are breeding grounds for traffickers to prey upon some of the most vulnerable, available and desirable victims. Cybersex trafficking involves the repeated abuse of children over video live feed to buyers on the other end of a webcam or cell phone, with victims experiencing isolation and humiliation. Buyers are predominantly from Western countries, often paying more money for material with increased violence and disturbing cruelty.[19] Unlike street brothels and bars, where victims are identifiable from the street and mainly serve local or visiting clientele, cybersex victims are exploitable anywhere, at any time and to thousands simultaneously.[20]

FOSTA/SESTA AND THE CHALLENGES OF CONTENT MODERATION

In recent years, the US Congress has sought to address online human trafficking through legislation, most notably Fight Online Sex Trafficking Act (FOSTA–SESTA). FOSTA–SESTA introduced by the House of Representatives and Stop Enabling Sex Traffickers Act, introduced by the Senate, created an amendment to the Communications Decency Act Section 230 of 1996.[21] Originally designed to address the role of online advertisements in soliciting the services of trafficked victims through website companies such as Backpage and Craigslist, both notorious for complicity in the trafficking of people, FOSTA–SESTA created a civil and criminal liability for online content providers for trafficking content on their services. These companies are forced to respond in one of four ways:

1. To avoid expensive lawsuits, make certain areas of their sites unavailable to avoid the problem altogether (for example, Craiglists shut down their personal ads page);
2. Shut down their website altogether and stop offering services and products;[22]
3. Choose not to set up monitoring and disrupting to avoid ‘knowingly’ hosting trafficking content; or
4. Monitor the activities of their users and actively remove potentially damaging content (for example, Google and Reddit both began removing some content that was potentially damaging).

Without robust cyber security strategies to combat these non–traditional cyber adversaries, or the proper incentives to do so, most online content providers were unable to select the most responsible option, the one the US Congress most hoped to force: option 4. Further unintended consequences of FOSTA–SESTA included the difficulty law enforcement faced trying to identify traffickers and victims via their online advertisements, the inability for service providers to reach potential victims online to offer services, trafficking content moving to the deep and dark web where it was more difficult, expensive and resource and expertise intensive to access and interdict and the shift of content overseas, often in the Netherlands, out of the reach of law enforcement subpoena or directives in some cases. Some of these consequences were short–term, others still remain in effect. Furthermore, sex worker advocates have argued that taking down such websites also left consensual sex workers more vulnerable. Without the means for them to screen potential clients, sex workers were forced to accept clients they may not have otherwise taken.[23]

Furthermore, online content providers are now faced with the dual challenges of how to moderate potential trafficking content in a legally compliant way that reduces their civil and criminal liability and also protects worker well–being.

Online content providers have struggled with high turnover rates and litigation from content moderation employees’ contractors. Of particular concern have been allegations of lack of support from employers regarding mental health protections, case studies on mental health impact and poor compensation relative to the horrific and oftentimes manual work required.[24] Content moderators are required to review thousands of abusive and egregious images, chat logs and other content and often face quotas on the number of cases they must review daily. From bullying to child rape, graphic violence to repeated sexual exploitation of minors, workers are bombarded with the worst of humanity with little to no reprieve or recourse. Some moderators with access to company-provided professional counsellors argue they receive advice and counsel that often benefits the employer and not the worker directly.[25] Companies turning to technical solutions, albeit at a slow rate, to address such issues are often hyper-focused on platforms using AI for photo recognition.[26] While a step in the right direction, relevant information connected to other potential trafficking cases is overlooked. Such information includes texts, phone numbers, geographic location, image metadata and latitude-longitude information. Without processing all available data, holistic measures are impossible to obtain.

Using cyber security techniques, however, including kill-chain analysis, ML, network interdiction and visualisation, consequence-driven analysis, threat modelling and detection- and defence-in-depth, online content providers can disrupt human trafficking processes, successfully moderate potential trafficking content and protect worker health.[27] The following study discusses how to successfully utilise cyber security techniques at scale.

ABILITY TO USE TECHNOLOGY FOR GOOD

Technological advancements are making promising strides towards identifying and disrupting human trafficking online and beyond. The human trafficking kill chain (see Figure 1), as developed by the Global Emancipation Network, offers a holistic approach to combating the issue. The kill chain represents a robust linear cognitive model for a complex, multidimensional crime to be used for effective decision-making in adversarial environments. The many stakeholders involved in counter-human trafficking efforts can benefit from applying this approach, ranging from law enforcement to commercial enterprises. A rigorous analytic framework such as the human trafficking kill chain enables users to recognise both data collection gaps and disruption opportunities that bring about the same end: increase the number of victims and traffickers identified and significantly decrease the amount of time it takes to do so. By automating much of the kill chain using analytics and other technologies, it frees up analysts to focus on the necessary elements that humans must do, such as public awareness campaigns, enacting legislation and conducting victim and trafficker interviews.

Figure 2 uses the terms *detect*, *deny*, *disrupt*, *degrade*, *deceive* and *destroy* to differentiate between possible options to weaken or destroy the adversary's ability to carry out their operations. It is important to note that these are ordered by the strength of the action and the amount of time the action has an impact on the adversary. A brief description and course of action for each is:

- *Detect*: Discover or identify the presence or existence of something. In tactical operations, detection is the perception of an object of possible military interest but unconfirmed by recognition. Similarly, in surveillance, detection is the determination and transmission by a surveillance system that an event has occurred. Example: run analytics on scraped posts advertising massage parlour jobs;
- *Deny*: Refuse to give or grant something to someone. A denial measure is an action to block the adversary's use of something necessary for operations. Example: block credit card purchases;
- *Disrupt*: Interrupt an event, activity or process by causing a disturbance or problem. By disrupting an adversary's operations, one creates a short-term stoppage. Example: ban a contractor

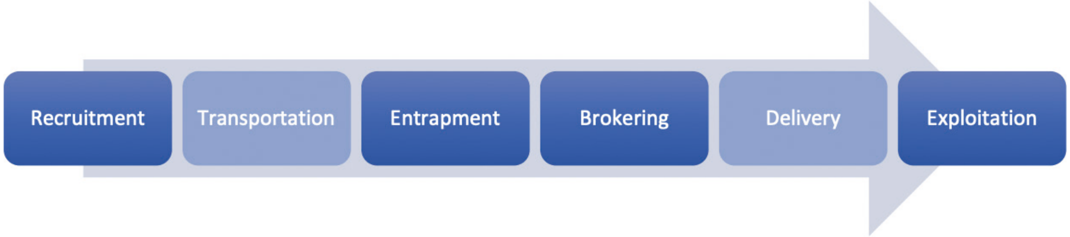


Figure 1: The human trafficking kill chain methodology
Source: Author

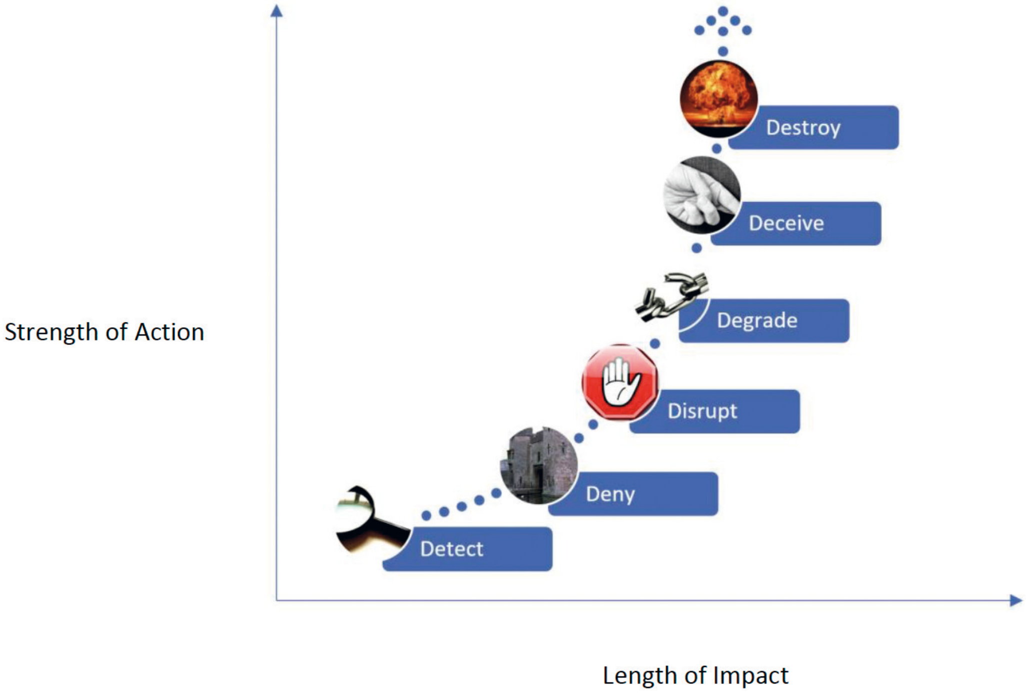


Figure 2: This shows the permanency of possible actions across the kill-chain spectrum
Source: Author

on H1-B visa applications for labour violations;

- *Degrade*: Lower the character or quality of something or someone; break down or deteriorate; reduce in amount, strength or intensity. By degrading an adversary's capabilities, one may also reduce their freedom of movement. Example: flood trafficking pages with false ads;
- *Deceive*: Cause someone to believe something that is not true, typically to gain an offensive or defensive advantage. Example: understate your technological capabilities during a public interview;
- *Destroy*: Put an end to the existence of something or someone by damaging or attacking it. To destroy, one creates a situation whereby the adversary has no means of recovery for a long period of time. Example: secure convictions and lengthy prison sentences for leaders of an international organisation.

The value of applying a kill-chain approach to human trafficking is automating as much of the process as you can to reduce time to value. It also highlights potential disruption strategies and combinations of courses of action to have the strongest, longest-lasting effect. Potential disruption options also vary by stakeholder.

Case study: The illicit massage industry

The illicit massage industry (IMI) is a network of illicit massage businesses (IMB) acting as fronts for commercial sex that operate as legitimate massage businesses across the world. Polaris and Praesidium Partners estimate there are over 10,000 such IMBs in the US alone.[28] These businesses line the busiest streets of major cities and dot strip malls across the US. Advertisements and reviews of services are often made via online platforms,[29] organising the 'best' places to hit for customers. As Polaris writes in its recent report entitled 'Human Trafficking in Illicit Massage Businesses':

> 'The sheer number of fake massage businesses, coupled with the impunity with which they operate, has over time fostered widespread – if tacit – cultural acceptance of the industry. The frequent wink, wink, nudge, nudge references to "happy endings," in popular culture is just one manifestation of perception that while commercial sex is illegal, in this context, it is essentially harmless. That perception is wrong. There may be women who choose to sell sex either along with or under the guise of massage therapy, but evidence suggests that many of the thousands of women engaging in commercial sex in IMBs or "massage parlors" are victims of human trafficking.'[30]

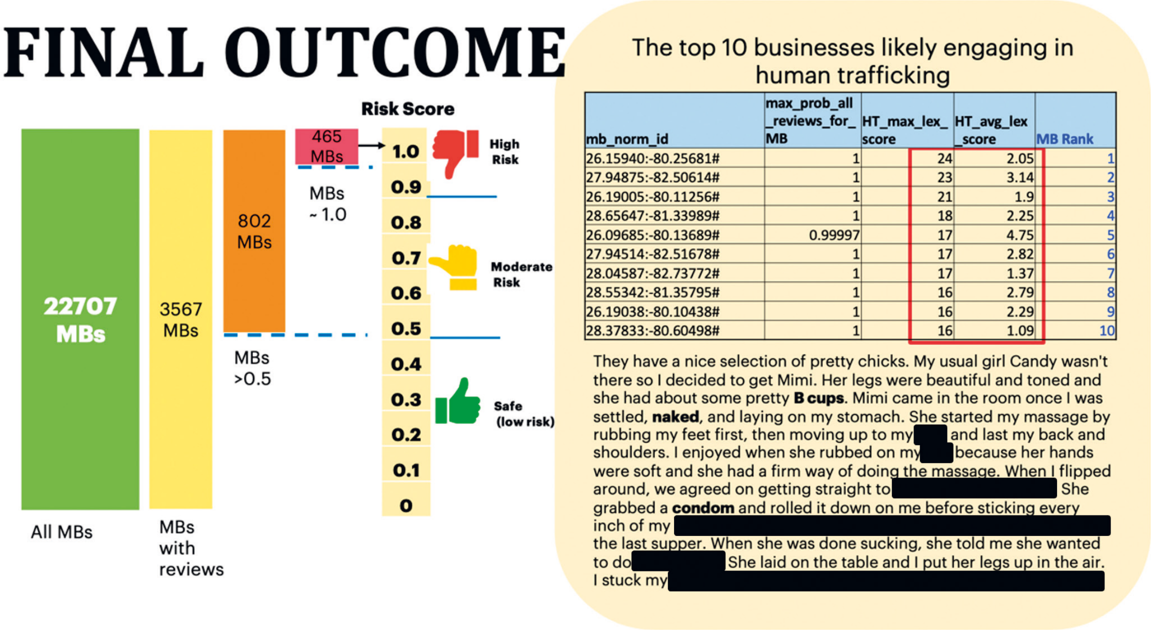
Global Emancipation Network,[31] Accenture Applied Intelligence,[32] Splunk for Good[33] and Graphistry[34] partnered to aggregate and correlate large sums of disparate data, test ML models and develop advanced analytics to create a proof of concept solution, Artemis. Artemis is a proactive, automated solution for counter-human trafficking stakeholders to increase efficiency on investigations and disruptions by identifying high risk establishments and individuals. The initial pilot focused on the IMI in the state of Florida, categorising massage businesses based on customer activity, staffing, location, services offered, imagery and disciplinary actions. Using this data and advanced analytics, Artemis creates risk scores and tiers for targeted action.

Artemis identified 22,708 unique massage businesses in Florida. Researchers focused on the 3,567 of those businesses that had or have customer reviews on either Rubmaps, an illicit massage review forum, or Yelp. Based on a lexicon of massage-centric sex terminology and related human trafficking terminology, 465 businesses scored 1, suggesting a 100 per cent likelihood the business is engaged in human trafficking. The top 10 offending businesses averaged 16 or more human trafficking-related terms in reviews, with the top offender racking up an average of 24 such terms per review. Artemis additionally identified 27 individuals operating illicit massage businesses as part of Florida trafficking networks, confirmed through manual analysis (see Figures 3, 4 and 5).

The National Science Foundation has provided a grant to support further data collection and analysis for Artemis, expanding into New York, Washington DC, Texas and California. In next iterations, researchers will focus on scalability, increased efficiency in correlating businesses, geospatial analysis, image and video analysis and improved optical character recognition (OCR) techniques, and then expand into content moderation on social media platforms, automated classification in the financial sector and additional verticals until Artemis represents a robust, automated and universal human trafficking classifier.

CONCLUSION AND RECOMMENDATIONS

Human trafficking is a pervasive issue exacerbated by the usage of technological



The top 10 businesses likely engaging in human trafficking

mb_norm_id	max_prob_all_reviews_for_MB	HT_max_lex_score	HT_avg_lex_score	MB Rank
26.15940:-80.25681#	1	24	2.05	1
27.94875:-82.50614#	1	23	3.14	2
26.19005:-80.11256#	1	21	1.9	3
28.65647:-81.33989#	1	18	2.25	4
26.09685:-80.13689#	0.99997	17	4.75	5
27.94514:-82.51678#	1	17	2.82	6
28.04587:-82.73772#	1	17	1.37	7
28.55342:-81.35795#	1	16	2.79	8
26.19038:-80.10438#	1	16	2.29	9
28.37833:-80.60498#	1	16	1.09	10

They have a nice selection of pretty chicks. My usual girl Candy wasn't there so I decided to get Mimi. Her legs were beautiful and toned and she had about some pretty **B cups**. Mimi came in the room once I was settled, **naked**, and laying on my stomach. She started my massage by rubbing my feet first, then moving up to my [redacted] and last my back and shoulders. I enjoyed when she rubbed on my [redacted] because her hands were soft and she had a firm way of doing the massage. When I flipped around, we agreed on getting straight to [redacted] She grabbed a **condom** and rolled it down on me before sticking every inch of my [redacted] the last supper. When she was done sucking, she told me she wanted to do [redacted] She laid on the table and I put her legs up in the air. I stuck my [redacted]

Figure 3: Highlighting the textual reviews on which Artemis operated, scoring reviews and businesses 0–1 based on a weighted lexicon. On the left, MB refers to massage business; 22,707 massage businesses were examined in total and 3,567 with reviews were selected for analysis with Artemis; 465 massage businesses rated a 1 or almost certain to be engaging in human trafficking
Source: Author

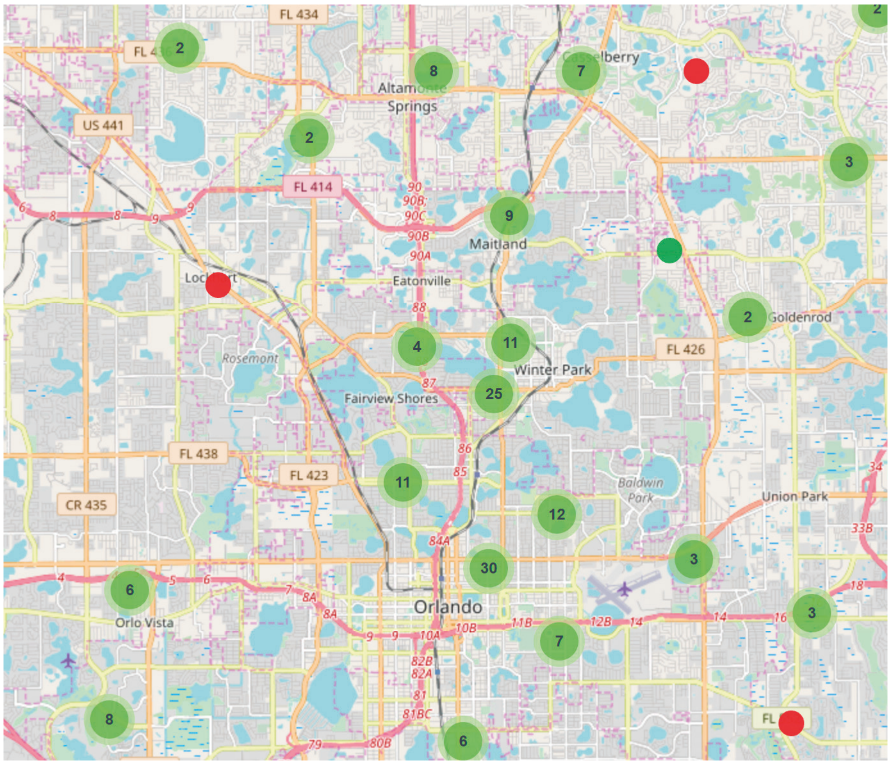
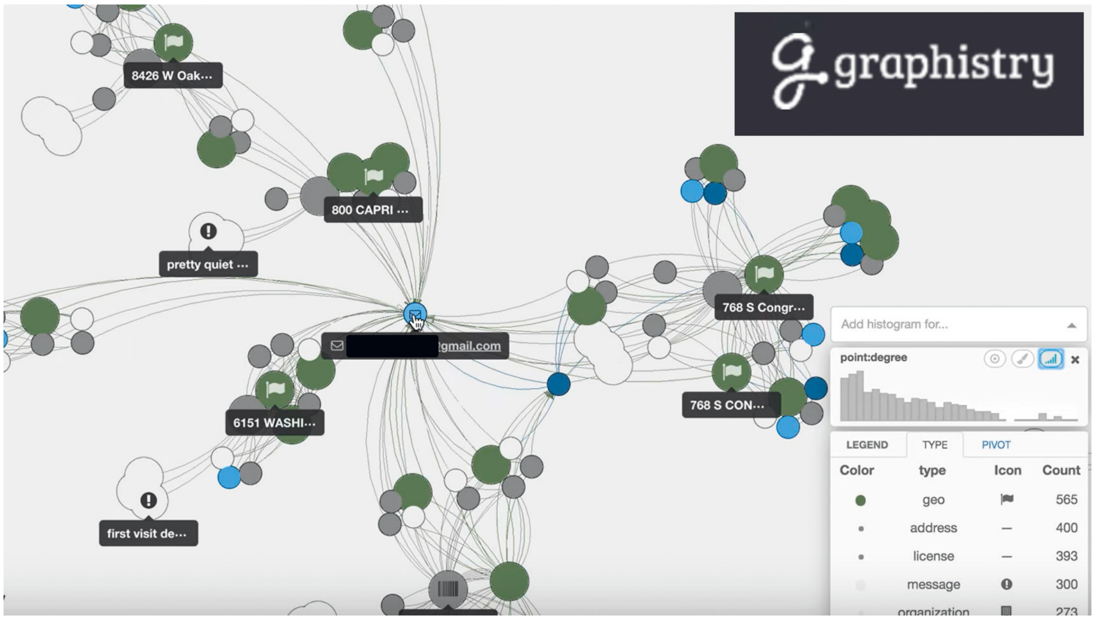


Figure 4: Cut-out of the Orlando, Florida area. Plotted are legitimate massage businesses in green and illicit massage businesses in red
Source: Author



Color	type	Icon	Count
●	geo	⚑	565
•	address	—	400
•	license	—	393
	message	❗	300
	organization	▦	273

Figure 5: Graphistry provides network analysis and graph GPU capabilities to Artemis. Here, individual phone numbers, usernames, addresses, e-mail addresses and reviews are clearly related, suggesting organised crime
Source: Author

developments for criminal enterprises. Promising methodologies such as the trafficking kill chain and technological advancements, such as Artemis, bridging collaborative efforts between stakeholders are keys for disruption. Moving forward, collaboration, centralisation of data and holistic legislation are critical ingredients for increased, effective anti-trafficking measures. Below, the aforementioned recommendations are discussed in brief:

1. Data collection geared towards human trafficking is often performed via individual organisations and/or agencies focusing on unscalable approaches. Data is often one or two targets deep, with a focus on superficial information that lacks connection to larger crime. Through a centralised approach, data would be standardised via a lexicon of words, images and numbers. Shared data would also allow for deeper connections providing layers to current trafficking patterns that can be disrupted and further prevented;
2. Expand the stakeholders involved in counter-human trafficking efforts beyond law enforcement, government agencies and non-profit organisations. Include private sector groups from finance, transport, agriculture, innovation and hospitality. Each of these sectors often encounters victims of traffickers within their sphere as well as collecting data and metrics that may illuminate trafficking patterns. By expanding the stakeholder circle and combining relevant data, trafficking becomes easier to spot. To ensure such participation, grantors and philanthropists should require stakeholder collaboration and contribution as part of any financial offering;
3. Expand beyond law and policy approaches that seek to remove content, including data that shows either intent or possible evidence and pursue legislation that empowers stakeholders to collect, manage and share data in preparation for counter-trafficking disruption; and
4. Develop and expand legislation and policies that require mandatory supply

chain audits and public disclosure for all companies, but especially those with international supply chains.

Notes and References

1. International Labor Organization (ILO) (2017), 'Global Estimates of Modern Slavery Forced Labour and Forced Marriage', Geneva, available at https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_575479.pdf (accessed 18th May, 2020).
2. Farley, M., Cotton, A., Lynne, J., Zumbeck, S., Spiwak, F., Reyes, M. E., Alvarez, D. and Sezgin, U. (January 2004), 'Prostitution and Trafficking in Nine Countries', *Journal of Trauma Practice*, Vol, 2, Nos. 3–4.
3. United Nations Security Council (2019), 'Identifying and Exploring the Nexus Between Human Trafficking, Terrorism, and Terrorism Financing', Counter-Terrorism Committee Executive Directorate, p. 60, available at https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf (accessed 18th May, 2020).
4. Organization for Security and Co-operation in Europe (2000), 'Protocol to Prevent, Suppress and Punish Trafficking in Persons, Supplementing the United Nations Convention Against Transnational Organized Crime', p. 12, available at https://www.osce.org/odihr/19223 (accessed 18th May, 2020).
5. United States Department of State Office to Monitor and Combat Trafficking in Persons (2019), 'Trafficking in Persons Report', available at https://www.state.gov/reports/2019-trafficking-in-persons-report/ (accessed 18th May, 2020).
6. United Nations Office on Drugs and Crime (2009), 'Global Report on Trafficking in Persons: Human Trafficking. A Crime That Shames Us All', p. 292, available at https://www.unodc.org/documents/Global_Report_on_TIP.pdf (accessed 18th May, 2020).
7. Pew Research Center (March 2014), 'World Wide Web Timeline', available at https://www.pewresearch.org/internet/2014/03/11/world-wide-web-timeline/ (accessed 18th May, 2020).
8. Clement, J. (July 2019), 'Internet usage worldwide – Statistics & Facts', Statista, available at https://www.statista.com/topics/1145/internet-usage-worldwide/ (accessed 18th May, 2020).
9. Clement, J. (December 2019), 'Number of internet users in the United States from 2017 to 2023 (in millions)', Statista, available at https://www.statista.com/statistics/325645/usa-number-of-internet-users/ (accessed 18th May, 2020).
10. Hughes, D. (July 2010), 'Sex Trafficking of Women for the Production of Pornography', *Citizens Against Trafficking*, p. 2, available at https://www.academia.edu/4847671/Sex_Trafficking_of_Women_for_the_Production_of_Pornography (accessed 18th May, 2020).
11. Keller, M. (September 2019), 'The Internet is Overrun with Images of Child Sexual Abuse: What Went Wrong?', *New York Times*, available at https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (accessed 18th May, 2020).
12. ECPAT International (2016), 'What We Do', available at https://www.ecpat.org/what-we-do/ (accessed 18th May, 2020).
13. BBC (October 2019), 'Dark web child abuse: Hundreds arrested across 38 countries', available at https://www.bbc.com/news/world-50073092 (accessed 18th May, 2020).
14. National Center for Missing and Exploited Children (2013), 'The Issue: Sextortion', available at http://www.missingkids.com/theissues/sextortion (accessed 18th May, 2020).
15. National Center for Missing and Exploited Children (2017), 'Executive Summary: The online enticement of children', available at http://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Exe%20Summary.pdf (accessed 18th May, 2020).
16. National Center for Missing and Exploited Children (2017), 'The Issues: The Online Enticement of Children: An In-depth analysis of CyberTipline Reports', available at https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf (accessed 18th May, 2020).
17. McDonald, S. (March 2019), 'Facebook sued by underage sex trafficking victim', Newsweek, available at https://www.newsweek.com/facebook-sued-underage-sex-trafficking-victim-1352953 (accessed 18th May, 2020).
18. International Justice Missio (2016), 'IJM Casework Series: Cybersex Trafficking', available at https://www.ijm.org/sites/default/files/IJM_2016_Casework_FactSheets_CybersexTrafficking.pdf (accessed 18th May, 2020).
19. *Ibid*., note 18.
20. Farley, M., Franzblau, K. and Kennedy, A. (2013), 'Online prostitution and trafficking', Prostitution Research, available at http://prostitutionresearch.com/wp-content/uploads/2014/09/FarleyFranzblauKennedyOnlineTrafficking-2014.pdf (accessed 18th May, 2020).
21. Wagner, A., Clarke, Y., Poe, T. and Maloney, C. (2018), 'H.R.1865 – Allow States and Victims to Fight Online Sex Trafficking Act of 2017', Version No. 6, p. 4, 115th United States Congress, available at https://www.congress.gov/115/plaws/publ164/PLAW-115publ164.pdf (accessed 18th May, 2020).
22. For example see Backpage, available at http://backpage.com/ (accessed 18th May, 2020).
23. Kessler, G. (August 2018), 'Has the sex-trafficking law eliminated 90 percent of sex-trafficking ads', WaPo, available at https://www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/ (accessed 18th May, 2020).
24. Garcia, S. (September 2018), 'Ex-Content Moderator Sues Facebook, Saying Violent Images Caused Her PTSD', *New York Times*, available at https://www.nytimes.com/2018/09/25/technology/

facebook-moderator-job-ptsd-lawsuit.html (accessed 18th May, 2020).

25. Newton, C. (February 2019), 'The trauma floor: The secret lives of Facebook moderators in America', The Verge, available at https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (accessed 18th May, 2020).
26. Jee, C. (November 2019), 'This is how Facebook's AI looks for Bad stuff', MIT Technology Review, available at https://www.technologyreview.com/f/614774/this-is-how-facebooks-ai-looks-for-bad-stuff/ (accessed 18th May, 2020).
27. Caltagirone, S., Laber, E., Yeng, S. and Wang, L. (August 2019), 'Sex Trafficking Detection with Ordinal Regression Neural Networks', *Machine Learning Journal.*, available at https://arxiv.org/pdf/1908.05434.pdf (accessed 18th May, 2020).
28. Keyhan, R. (2018), 'Human trafficking in illicit massage businesses', Polaris Project, available at https://polarisproject.org/sites/default/files/Full_Report_Human_Trafficking_in_Illicit_Massage_Businesses.pdf (accessed 18th May, 2020).
29. Such as Rubmaps.com. Note: Rubmaps.com has been moved to Rubmaps.ch in an effort to elude authorities (accessed 1st June, 2020).
30. *Ibid*., note 28.
31. Global Emancipation Network (GEN) is a global data analytics and intelligence non-profit dedicated to counter all forms of human trafficking, the second most profitable and fastest growing crime across the world. Minerva, the multi-tenant data analytics and investigations platform created and hosted by GEN, empowers users across the counter-trafficking stakeholder community to find trafficking victims, stop traffickers and inform resource allocation and policy.
32. Accenture Applied Intelligence helps clients apply new data science and intelligent technology across their business, and into every function, so they can transform their business and achieve new outcomes at speed and scale. Recognised as a leader by industry analysts, the company helps clients create new intelligence using AI, ML, proprietary algorithms and app-based solutions, all powered by the Accenture Insights Platform. Accenture collaborates with a powerful alliance and delivery network to help clients operationalise within any market and industry with a focus on speed to value. Combining expertise across industries, analytics, technology and design, Accenture is uniquely qualified to drive new business outcomes with precision, at scale.
33. Splunk believes that data can make for better business and a better world. Splunk for Good, Splunk's charitable arm, works to inspire action and create opportunity through people, partners and data. Splunk partners with organisations at the local, state and federal levels to leverage data in support of initiatives such as disaster and humanitarian response, counter-human trafficking, and open government. Through a US$100m Splunk Pledge, the company supports nonprofits, workforce training, research and education through product donations, discounts and education to provide access to exciting new career opportunities. The US$50m Social Impact Fund invests in early stage organisations that are using innovative, data-driven approaches to drive meaningful social impact.
34. Graphistry unlocks the potential of data by turning raw records into highly visual and interactive incident maps. The graph-based analysis reveals hidden connections and context across all provided data, and within seconds lets analysts see key relationships, event scope and progression, patterns and anomalies, all without writing a manual query or tabbing between tools. Additional easy drill downs and pivoting on the fly allow for streamlined investigations and analysis.