CSSF Women, Peace and Security Helpdesk

Beyond the Binary: Dynamics of Gender, Serious and Organised Crime and Artificial Intelligence

Submitted: 28/03/24

Assignment Code: WPS065

WPS Women, Peace & Security Helpdesk

The Women Peace and Security Helpdesk, managed by Saferworld in partnership with Conciliation Resources, GAPS UK, University of Durham and Women International Peace Centre (WIPC), was established in December 2021 to increase capability across the UK Government on WPS policy and programming in order to make its work on conflict and instability more effective. If you work for the UK government and you would like to send a task request, please email us at wpshelpdesk@saferworld.org.uk. If you do not work for the UK government but have an enquiry about the helpdesk or this report, please email us at enquiries.wpshelpdesk@saferworld.org.uk.

Experts: Eleonore Fournier-Tombs

Direct Audience: FCDO Serious and Organised Crime (SOC) Unit, National Security Directorate

Suggested Internal Distribution: FCDO Teams working on AI and SOC

Confidentiality Status: Open source

UK Government

UKaid
from the British people

Table of Contents

1. Executive Summary

Overview

The effect of new artificial intelligence (AI) developments, particularly generative AI, on serious and organised crime (SOC) have been significant over the last few years. Analysed with a gender lens, these effects can be nuanced and complex, ranging from changes in patterns of victimisation to new opportunities and pitfalls in crime prevention. Women's participation in SOC is changing as well, as AI increases certain vulnerabilities while providing novel mechanisms for criminal participation.

As AI governance efforts at all levels of government are increasing—from national regulatory and standard-setting efforts in many countries, to multilateral and multistakeholder United Nations-led processes—establishing a better knowledge base for these issues can aid in the development of much more appropriate policies. This report builds upon the gender dynamics of victims and offenders in SOC, as well as recent research on the gender risks of AI—discrimination, stereotyping, exclusion, and insecurity.

AI tools are used increasingly in both enabling and combatting gender-based crime. For example, AI has been used to conduct selective victimisation and optimise human trafficking. It has also been used in several novel virtual crimes, such as non-consensual deepfake pornography, extortion and psychological manipulation, impersonation and identity theft, doxing and stalking, where women and girls, especially those from marginalised groups, are disproportionately affected (UN Women, 2023). The gender risks of AI more generally threaten to unintentionally increase women's vulnerability to crime, for example, making them less able to participate in the labour force, reducing their ability to receive loans, and causing them many other forms of socioeconomic insecurity.[1]

There are also gender risks in the exploitation of AI tools themselves by criminals. Techniques can include AI algorithm poisoning, hacking of AI systems to steal sensitive personally identifiable information, stalking women, or sabotaging AI safety systems. AI algorithm poisoning, in particular, can increase bias in AI systems, leading to outputs that foster gender stereotypes or misogyny.

AI has been used in many instances to combat trafficking and the physical exploitation of women, as well as protect women from virtual exploitation. There are many examples of chatbots providing support to women victims, police forces using predictive policing, and data fusion tools enabling the tracking of suspicious travel, sharing of images of children, and other criminal activity. These uses of AI, which can both enable gender threats in SOC or combat them, can have broader secondary effects. Notably, these are seen in policing, in the changing roles of women participating in SOC, and in transnational crime.

Police forces have adopted a number of AI tools to increase the efficiency of their work. These include body cameras with facial recognition systems, crowd surveillance systems, and predictive policing tools. The possibility of bias in these tools is well documented,[2] with women of colour most likely to be victims of misidentification or other bias. Other concerns include the risk of over policing or bias confirmation in lower income areas or with certain types of minor crime.

[1] See: Fournier-Tombs, E. (2023b). *Gender Reboot*. London: Palgrave MacMillan.

[2] See, for example: Brayne, S. (2020). *Predict and Surveil: Data, discretion, and the future of policing*. Oxford University Press, USA.

The effect of AI on SOC as an illegal economic sector may also change the role of women as offenders. Women have historically participated in SOC in many different roles, especially in certain sectors, such as human trafficking and money laundering (UNODC, 2022). However, they have been in the minority, with several research reports citing their participation being approximately 10 per cent of offenders. Part of this was due to stereotypes, which women have sometimes been able to use to their advantage, but part was also due to the physical nature of the criminal work. With AI, cybercrime is now rising, which can mean increased participation for women if they gain technical skills. The Japanese cybersecurity firm Trend Micro (2021) published a detailed analysis of women's participation in cybercrime, which includes an estimation that 30 per cent of cybercriminal forum participants are women, as well as some evidence that women are increasing their participation in cyber criminality.

Finally, AI has contributed to the growth of transnational crime, particularly due to its utility in cybercrimes, which are by nature transnational. Increasingly, criminals can commit crimes with international reach. Certain sectors seem particularly affected by an increase in transnational crime: cyber exploitation and financial fraud, money laundering, non-consensual pornography and deepfake content creation, and cybersecurity. AI has also been used by transnational actors to generate and disseminate disinformation, leading to violence, particularly when seeking to destabilise another country and manipulate public discourse (Albrecht et al, 2024).

However, understanding the effects of AI on transnational crime and other types of SOC is challenging. An important factor, according to the findings of this report, is the paucity of data collection about women and SOC. Although there are some estimates about women as victims and offenders, often data is not disaggregated by gender. The risk of AI adoption in the sector is also, therefore, that anonymity of offenders and victims will further reduce the data available on women and SOC.

In light of this, this report makes the following policy and technical recommendations, which aim to address risks of AI from a gender perspective, propose ways of better harnessing its opportunities for combatting crime and protecting women, and solve some of the important data gaps in this domain.

Summary of Recommendations

Policy Recommendations

1. Women, Peace, and Security (WPS) and SOC policy forums share common concerns regarding AI and women's safety. It would be relevant to use future opportunities, such as the Commission on the Status of Women, to initiate a common effort to add to the global governance instruments in each case; for example, the WPS Agenda and the Palermo Protocols.[3]

2. Ongoing national and global AI governance processes should mainstream gender considerations, which could include the collection of gender-based data for all AI risks and opportunities.

3. National governments should ensure that AI used in policing is properly audited and regularly revisited, with different strategies used for day-to-day policing of minor offences versus larger transnational efforts.

4. National governments should prioritise investing in responsible AI tools to combat gender-based criminal victimisation, especially to understand the phenomenon and address it in policy.

[3] For a nuanced analysis of the way in which the Palermo Protocols could better include new technologies, see: Zinser, S., & Thinyane, H. (2021). A Step Forward for Palermo's Trafficking Protocol, This Time Integrating Frontier Technology. *Yale J. Int'l Aff.*, *16*, 140.

Technical Recommendations

1. Generative AI companies should prioritise eliminating stereotyping and discrimination in their tools, which can have significant effects on the systemic vulnerability of women, notably by conducting gender impact assessments *before* deployment.

2. Technical standards used by AI companies, such as the United States-based National Institute of Standards and Technology standards, should include gender and SOC impact assessments that all public-facing tools should conduct before deployment.

3. All AI companies, with a focus on generative AI companies and social media platforms, should further prioritise reducing misuse of their tools, by developing much better guardrails for women's protection before the tools are deployed, especially in non-English languages and varied cultural contexts.

2. Findings and Analysis

Introduction

The advent of new artificial intelligence (AI)[4] technologies is almost certain to transform the landscape of serious and organised crime (SOC),[5] introducing both novel challenges and opportunities. Responding to this technological shift requires a nuanced understanding of gender[6] and crime, spanning not only the impact of crime on women and girls but also the role of both men and women in organised crime. AI technologies, especially those used in large-scale data analysis and predictive modelling, offer unprecedented tools for criminal enterprises, optimising everything from trafficking routes to sophisticated cybercrimes. Those same technologies also allow for increasingly granular mechanisms for identifying criminals and protecting victims.

The gendered impact of SOC, often underexplored, reveals a complex pattern of victimisation and participation. Women and girls, traditionally underrepresented in the technology industry, find themselves disproportionately affected by new technologies as victims of AI-enabled crimes, such as digital harassment or sex trafficking (European Institute for Gender Equality, 2017). Conversely, the evolving nature of organised crime, underpinned by AI, presents new roles that may disrupt traditional gender norms within these illicit networks. This duality underscores the necessity to integrate a gender-sensitive lens in the study of AI's role in SOC, acknowledging both the gendered patterns of victimisation and the potential for subverting entrenched gender roles within criminal hierarchies.

As highlighted in the United Kingdom (UK) Government's 2023 White Paper on international development, transnational crime is growing significantly, partly due to advances in new technologies that have eased a path for distributed crime networks and virtual crime. The paper also outlines tackling online gender-based violence as a priority for reaching Sustainable Development Goal 5 (Achieve gender equality and empower all women and girls) by 2030 and calls for multilateral action to address harmful content and sexual exploitation (HM Government, 2023). Current efforts in AI governance at the national and global level could benefit from incorporating considerations of SOC and gender, which could have important implications for their structures and processes.

This paper examines the relatively under-explored dynamics of AI, SOC, and gender, particularly to understand potential impacts on gender issues in relation to the emergence of AI-facilitated organised crime. This research is based on a review of literature conducted in January and February 2024. The paper is informed by recent developments in AI technologies, such as the deployment of generative AI tools. Although this research hopes to be forward-thinking, it may require updating as the AI and SOC fields evolve.

[4] The Organisation for Economic Co-operation and Development's (OECD) latest definition of AI has been widely adopted. It reads as follows: "An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment" (OECD, 2023).

[5] SOC is defined by the UK government as: "individuals planning, co-ordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks." The categories of SOC covered under this definition are child sexual exploitation and abuse; illegal drugs; illegal firearms; fraud; money laundering and other economic crime; bribery and corruption; organised immigration crime; modern slavery and human trafficking; cybercrime (UK Government, n.d.).

[6] UN Women defines gender as: "the social attributes and opportunities associated with being male and female and the relationships between women and men and girls and boys, as well as the relations between women and those between men" (UN Women, n.d.).

Conceptual Framework

2.1 Understanding Gender in SOC

Although women are more likely considered to be victims than offenders in crime, the reality is more nuanced. United Nations (UN) Women, in a report on gender and technology-facilitated violence, highlights a lack of understanding and data on the topic, which makes it difficult to report on accurately (UN Women, n.d. b).

In 2020, the United Nations Office on Drugs and Crime (UNODC) published a thematic note on gender mainstreaming in organised crime and illicit trafficking. The note called for distinct consideration in approaching victims and offenders based on their gender, with certain crimes more likely to involve women and girls (UNODC, 2020). In such cases, especially in human trafficking, it is important to consider the victim–offender overlap, where women who may originally have been victims maintain a relationship with the criminal organisation as offenders (Kotarska, 2023).

Gender and criminal victimisation

Women, as a demographic group, are disproportionately victimised in various facets of SOC, a pattern evident across diverse geographical regions. Predominantly, the sectors of organised crime where women are most vulnerable include human trafficking, sexual exploitation, and increasingly, technology-driven crimes such as cyberstalking, identity theft, and online harassment.

Statistics reveal that women are at higher risk of human trafficking, with a notable likelihood in regions marked by socioeconomic disparities and weak law enforcement. The victims predominantly include those from vulnerable sections, including minorities, those in poverty, and individuals in areas with high rates of crime. The organisation Stop the Traffik, for example, reports that 71 per cent of trafficking victims around the world are women and girls, while 29 per cent are men (Stop the Traffik, n.d.). UNODC also reports that 2 per cent of those trafficked are of transgender or non-binary identity. Additionally, of those that are trafficked, statistics show that men and boys are more likely to be trafficked for forced labour, while women and girls are more likely to be trafficked for sexual exploitation (UNODC, 2022). In its latest Global Report on Trafficking in Persons, UNODC reports that women are three times more likely to suffer violence at the hands of traffickers than men (UNODC, 2022).

As early as 2017, the European Institute for Gender Equality reported cyber-enabled crime as a growing threat for women, with women and girls representing over 90 per cent of non-consensual pornography victims (EIGE, 2017). In recent years, journalists, women in public life, and women human rights defenders have been targeted regularly by cyber-enabled crime, notably with the intent of silencing them (UNESCO, 2021). This threat has grown considerably over the last two years, not only in relation to non-consensual pornography but also in relation to fraud, data theft, and cyberstalking. Burgess reports that in 2023, there was a 50 per cent increase in the number of deepfake pornographic videos[7] compared to 2022, with the ease and accessibility of generative AI technologies cited as a primary cause (Burgess, 2023).

New advances in AI have ushered in new avenues for criminal activities, where women are specifically targeted through means like non-consensual dissemination of sexual images, cyberbullying, and exploitation via online platforms. These modern crimes add a layer to traditional forms of exploitation, requiring a more nuanced understanding and specialised strategies for prevention and protection.

[7] Burgess conducted a study of 35 websites hosting deepfake videos, noting 73,000 videos uploaded in 2022 and 113,000 videos uploaded in 2023.

Women as offenders

Although women's roles as perpetrators of SOC are often underreported, there is evidence that women are increasingly taking part in crimes such as trafficking, terrorism, and money laundering.

Gender stereotypes, however, play an important role in the perceptions of women as offenders globally. The Organization for Security and Co-operation in Europe, in a report on gender roles in SOC, notes that women are "*perceived as passive, less violent and subject to the decision-making of men. This can allow them to act almost invisibly within OCGs [Organised Crime Groups], remaining undetected by criminal justice systems despite contributing to the criminal activities of these groups*." The report notes that, in fact, women are known to be active in organised crime groups, conveying messages to and from prison, managing trafficking or money laundering activities, or as professionals such as lawyers and accountants. They note that women often play an important role in socialisation around a criminal group, creating a sense of culture and influencing members to join (OSCE, 2023).

There is very little research available on the participation of women in cybercrime, technology-enabled crimes, or AI-facilitated crimes. In fact, exploration of several prominent research repositories, such as Google Scholar and JSTOR, primarily show articles highlighting the victimisation of women by AI-facilitated crime. However, this finding may hint at the lack of data and research on women and AI-facilitated crime, rather than the complete lack of participation of women in AI-facilitated crime. This possibility is supported by two secondary findings: first, that women's participation in SOC has increased over the last decade; and second, that AI technologies have broken down barriers to women's participation in other domains, such as e-commerce (Sadrul et al, 2023).

Nevertheless, according to UNODC (2022), data on the role of women as offenders is certainly inaccurate, notably biased by the fact that women, once investigated, are more likely to be prosecuted and convicted than men. In fact, although only 28 per cent of investigations of traffickers are targeted towards women, 41 per cent of convicted traffickers are female.

Victim–offender overlap

The phenomenon of victim–offender overlap presents a multifaceted issue, characterised by a pattern where victims of such crimes may transition into perpetrators, and is observed across genders. This dynamic is particularly pronounced in areas with entrenched socioeconomic challenges, where limited resources and systemic barriers often lead women, initially victims, to engage in criminal activities as a means of survival or coercion (Aronowitz & Chmaitilly, 2020). Women, especially those previously subjected to exploitation or abuse, may find themselves enmeshed in activities such as drug trafficking, fraud, or even becoming part of human trafficking networks.

The way in which AI has impacted gendered transitions between victim and offender, however, is still little known. Although Parti et al (2022) have documented this effect in both online and offline crimes, and note some transition between online and offline criminality, the implications of this for AI-enabled or combatted crimes would warrant further research.

2.2 Known Risks of AI to Women's Peace and Security

Separate from crime, there has also been growing research on the risks of AI to women, and particularly to women's peace and security, and the way in which these risks could impact women's socioeconomic vulnerability. In a forthcoming report, UN Women highlights five overlapping dimensions of risk of AI to the Women, Peace and Security (WPS) agenda: discrimination, stereotyping, feminisation, exclusion, and insecurity (UN Women, 2024, Forthcoming; Fournier-Tombs, 2023). These can be briefly defined as follows:

- *Discrimination*: When an AI tool has a different, inferior output for women than men, such as biased hiring tools that reject female candidates based on their gender (Zou & Schiebinger, 2018). The accumulation of discriminatory AI risks increasing the socioeconomic vulnerability of women, making them more vulnerable to crime.

- *Stereotyping:* When the AI tool assumes or propagates notions of the inferiority of women in relation to men, such as generative AI tools that create content that sexualises or degrades women (West, Whittaker, & Crawford, 2019). Exposure to stereotyping content can increase the acceptance of violence against women (Gavin & Kruis, 2022).

- *Feminisation:* When an AI tool is presented as having a female gender by default, as has been the case for many human–AI interfaces, such as virtual assistants (Apple's Siri; Microsoft's Cortana; Amazon's Alexa), robots (Sophia the Robot), and chatbots. These representations have been criticised for contributing to the objectification of women and putting them in a position of submissiveness and sexualisation, which could lead to increased acceptance of stereotyping and discrimination of women outside of AI (Strengers & Kennedy, 2021).

- *Exclusion:* When women are underrepresented in the design, development, and decision making around the tool, and are less likely to benefit from it (Fournier-Tombs & Castets-Renard, 2021). However, women-led AI development initiatives can help fight the victimisation of women (Quinn, 2019).

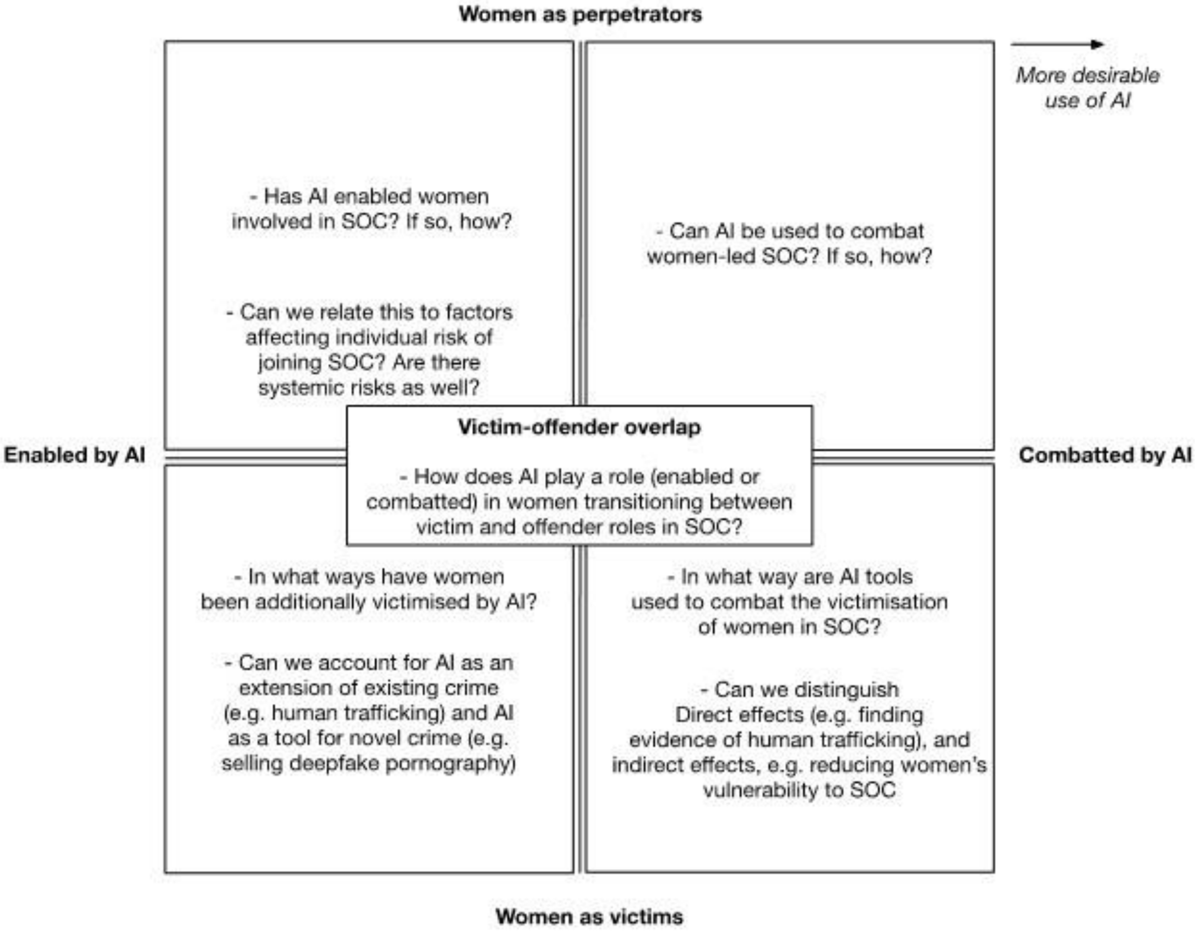
- *Insecurity:* When the AI tool reduces the physical or psychological safety of women, either in the online or offline sphere, such as ride-sharing applications that do not take women's security into account (Rosenblat & Stark, 2016).

These risks are applied separately from the intent of the AI tool developed. For example, even tools built in order to support peacebuilding, aid criminal investigation, or track victims of trafficking may have some of these risks if they are not mitigated at the design phase. As we will see, each one of these risks can increase women's vulnerability to victimisation or even participation in criminal activity.

2.3 A Framework for AI, SOC, and Women

The following diagram aims to clarify the multiple roles of women and the multiple uses of AI as they relate to this research. In each quadrant, we see the key research questions addressed in this report.

Figure 1: Conceptual framework for AI, gender, and SOC



Women as perpetrators
More desirable use of AI
- Has AI enabled women involved in SOC? If so, how?
- Can we relate this to factors affecting individual risk of joining SOC? Are there systemic risks as well?
- Can AI be used to combat women-led SOC? If so, how?
Enabled by AI
Combatted by AI
Victim-offender overlap
- How does AI play a role (enabled or combatted) in women transitioning between victim and offender roles in SOC?
- In what ways have women been additionally victimised by AI?
- Can we account for AI as an extension of existing crime (e.g. human trafficking) and AI as a tool for novel crime (e.g. selling deepfake pornography)
- In what way are AI tools used to combat the victimisation of women in SOC?
- Can we distinguish Direct effects (e.g. finding evidence of human trafficking), and indirect effects, e.g. reducing women's vulnerability to SOC
Women as victims

3. Research Results

SOC has been just as impacted by AI as other industries—legal or illegal. This means that AI has begun to have an impact not only on the organisation and activities related to SOC but also in the way in which SOC is combatted globally. Women are most often involved in drug trafficking, extortion and money laundering, and human trafficking (Enfield, 2019), both as victims and as perpetrators (GIWPS, 2020). The following section goes deeper into the effects of AI to enable and combat these types of crimes, with a gender perspective.

While every category of SOC has been affected by new AI developments, the impact of this on women is not homogenous. Broadly, the effects can be seen in AI being used to enable trafficking, smuggling, and enslaving women and girls; AI used to virtually exploit women and girls; AI to increase the vulnerability to crime of women and girls; and conversely, AI to combat the physical and virtual exploitation of women and girls. In addition, there is a gender dimension of AI as the target of criminal attacks, which is explored below.

In the table below, we outline some of the ways in which we can understand AI being used to enable or combat SOC, and what this could mean with a gender lens.

Table 1: Understanding the uses of AI in SOC

SOC category	*Enabled using AI*	*Combatted using AI*	*Gender lens*
Child sexual exploitation and abuse	Several organisations have reported the use of AI for the creation of sexual abuse imagery, the distribution and normalisation of sexual abuse imagery,[8] and targeting vulnerable children or increasing their vulnerability.	Tools used to fight child sexual exploitation include predictive policing, content moderation, tracking of suspicious behaviour, reporting suspicious behaviour, providing tools and advice for victims (chatbots).	The Internet Watch Foundation details over 11,000 AI-generated images of children, including sexual abuse, rape, and violence against small children.[9] 99.6 % of the images found in this study were of girls.
Illegal drugs	Recommendation systems and advertising, both of which use AI, facilitate the sale of drugs online. Other types of AI can be used to optimise drug trafficking routes, predict law enforcement patterns, and assist in the illicit production of drugs through chemical analysis.	Predictive analytics can anticipate trafficking routes and distribution networks and can also analyse drug trends to aid in prevention strategies.	There are gender differences in offenders and victims in the area of illegal drugs. As we see in Box 3, data gaps make it difficult to integrate these considerations in AI tools combatting drugs.
Illegal firearms	A concerning application of AI has been the development of autonomous weapons systems and armed drones, as well as the streamlining of illegal arms, trafficking logistics, or designing untraceable firearms, such as 3-D printed guns.	AI has been used to assist in tracing illegal firearms and analysing patterns in arms trafficking, leading to more effective crackdowns.	Women's involvement in arms trafficking is often overlooked. AI can help uncover these roles, leading to more comprehensive strategies against firearms trafficking.
Fraud	Generative AI used to conduct scams such as phishing attacks or various types of fraud.[10]	AI tools can detect fraudulent patterns and anomalies in financial transactions, aiding in fraud prevention and detection.	Men and women are targeted differently by fraud and blackmail. AI can help identify gender-specific fraud patterns.

[8] See: Dodd, V & Milmo D. (2023).

[9] Internet Watch Foundation (2023).

[10] See: United Kingdom Government (2024).

Money laundering and other economic crime	Automation of money laundering processes, illicit access of bank accounts that are then used in money laundering.	See EY report on AI for Anti-Money Laundering.[11] AI can analyse complex financial data to identify suspicious activities indicative of money laundering.	Gendered analysis can reveal how women might be uniquely involved in or affected by these crimes, allowing for tailored prevention and enforcement strategies.
Bribery and corruption	Data analysis can be used to find the most effective bribery targets or to hide corrupt transactions (AI anti-corruption tools).	AI can be used to detect patterns and anomalies indicative of bribery and corruption in large datasets, like government contracts.	Understanding gender dynamics in power structures can help AI tools better detect and combat gender-specific forms of corruption.
Organised immigration crime	AI can be used in the planning and execution of complex human smuggling operations.	AI can be used to aid in identifying smuggling routes, analysing migration patterns, and supporting victims.	AI is increasingly used in migration, including to recruit victims for smuggling. Due to the vulnerability of the migrants and to other gender risks of AI, this can put women and girls at even higher risk.
Modern slavery and human trafficking	AI is also used to recruit victims (notably with recommendation systems) and optimizing trafficking networks.	Predictive analytics can identify patterns indicative of trafficking, help in victim identification, and support rehabilitation efforts	While women and girls are at higher risk of being sexually trafficked, boys and men are more often trafficked for labour.[12] Gender data here can play an important role in understanding and combatting AI-enabled trafficking.
Cybercrime	AI tools, such as Generative AI tools, are increasingly used for hacking, phishing, and other cyber attacks, including attacks conducted in the virtual space, such as a metaverse, including in the online impersonation of police officers. In addition, the adoption of AI and digital tools can increase vulnerability to cyber attacks.	AI-driven cybersecurity can detect and prevent attacks, analyse cyber threats, and aid in the recovery from incidents.	Women are often targeted in specific cybercrimes like online harassment.[13] AI can help identify these gendered patterns and provide targeted protection.

3.1 Applications of AI in a SOC Context

In the section below, we go into further detail on applications of AI in a SOC context. It should be noted, however, that the extent to which AI is used in enabling and combatting crime is not always known. Many different types of algorithms are reported, from generative AI to recommendation systems, optimisation systems, and predictive analytics tools. Many AI tools might use a combination of algorithms, or may in fact not use AI at all but rather other types of digital technologies.

3.1.1 AI used in trafficking and exploitation

Selective victimisation emerges as a critical concern in the deployment of AI systems, which, due to biased data inputs, may inadvertently prioritise or neglect the protection of specific groups, notably women, thus exacerbating their vulnerability to SOC activities. Recent studies underscore this issue, with Buolamwini and Gebru (2018) documenting how facial recognition technologies have been less accurate in identifying women of colour. These errors have the potential to lead to lower rates of intervention in instances of trafficking. Similarly, Luengo-Oroz et al (2021) analysed the use of AI in COVID-19 services

[11] See, for example: EY (2023).

[12] UNODC (2022).

[13] UN Women (n.d. b) reports that in the European Union, 1 in 10 women has experienced cyber harassment since the age of 15, and that 60 per cent of women in Arab States has been exposed to online violence in the past year.

during the pandemic, finding that biases in these systems could lead to insufficient resources being directed towards women and minority groups, leaving them more exposed to exploitation and violence, including trafficking.

AI has also been used in the optimisation of human trafficking. Although research on technology-enabled trafficking is not as common as research on combatting trafficking with technology, researchers document social media algorithms in particular in the recruitment of victims and sale of their services. Raets and Janssens (2021), for example, explain how recommendation systems have been instrumental in the Belgian human trafficking business. This adoption of new technologies in criminal activities is not new. In an earlier study of India, Nepal, Thailand, Hungary, and the UK, Sarkar (2015) notes that "*traffickers and their networks made good use of sophisticated software in order to safeguard their anonymity, make use of online storage and hosting services, and use advanced encryption techniques to counteract digital forensic investigations by the police*."

The widespread adoption of AI and digital tools also inadvertently increases the susceptibility to cyberattacks; as we will see, biases in AI tools can increase the socioeconomic vulnerability of women and those from other marginalised groups. Additionally, one of the primary case studies explored by Caldwell et al (2020) in their research on AI-enabled future crime is AI-enabled blackmail. They highlight how phishing attacks and malware, often orchestrated with the assistance of AI, can compromise the digital identities of individuals, making women more vulnerable to blackmail and coercion into trafficking networks. Cho et al (2023), in a study examining 16 individual instances of deepfake videos, further elaborate on the use of deepfake technology to create compromising materials used to threaten and control victims, documenting a growing trend in cyber-enabled exploitation.

According to a report by University College London, fake audio or video content has been identified as a particularly worrying use of AI with potential applications for crime or terrorism. Deepfakes could be used to discredit public figures, manipulate elections, or even impersonate individuals for financial extortion—demonstrating the transnational implications of such technology. The difficulty in detecting and stopping such content could lead to a widespread distrust of audio and visual evidence, representing a significant societal harm (UCL, 2020).

An increasing concern, particularly with the ongoing rolling release of more and more powerful generative AI tools, is the creation and dissemination of non-consensual pornography, especially deepfake content (Chesney and Citron, 2019). This exploitation significantly impacts women's privacy and mental health, as these AI-generated images or videos can be almost indistinguishable from real footage, leading to widespread personal and professional consequences for the victims. From a criminal perspective, researchers have documented the growing use of AI-generated deepfake videos for blackmail and fraud in Asia (Dymples, 2022).

Notably, AI has been used to enable romance scams, which target both men and women. The McAfee study, 'Modern Love', which was conducted in seven countries globally, found a striking increase in generative AI use on dating applications for scamming purposes. It reports that nearly half of people on online dating sites have seen AI-generated profiles, and up to one third have been asked for personal information such as their social security number, phone number, address, and salary by would-be scammers (McAfee, 2024). The UK Revenge Porn Hotline reports that although women are more likely to be affected by intimate image abuse, men are five times more likely to be targeted in sexual extortion (Lofkin, 2023).

Moreover, AI algorithms can drive targeted extortion schemes and psychological manipulation tactics, often leveraging intimate or personal information against women. Such AI-enabled strategies not only breach privacy but also inflict severe emotional distress, manipulating victims into situations of helplessness and fear (Aiken, 2016). The automation of impersonation, identity theft, and the facilitation of stalking and doxing through AI-powered tools disproportionately target women, exacerbating the risks associated with online presence (Dunn et al, 2023). The production and distribution of deepfake pornography and AI-created sexual abuse imagery further illustrate the malicious use of AI to degrade and harm women, normalising sexual abuse imagery and contributing to a culture of exploitation and violence against women (Dunn et al, 2023; Fournier-Tombs, 2023b).

Box 1: Children and online sexual exploitation

Female traffickers have been found to take prominent roles in the sexual exploitation of children, notably in having them appear in livestream videos. The International Justice Mission's 'Scale of Harm' report shows that in 2022, one out of every 100 Filippino children was trafficked to produce sexual exploitation material, making it a global epicenter. While boys were also exploited, the majority of those trafficked were girls.

Traffickers were typically women and were known to the children, subjecting them to sexually violent acts or having them perform other kinds of sexual content. The report notes an increase in this type of trafficking in the last few years, with the widespread availability of video streaming services combined with post-pandemic economic challenges as primary contributing factors (International Justice Mission, 2023).

3.1.2 AI used to combat trafficking and exploitation

At the same time, AI has also increasingly been used to combat human trafficking, particularly through predictive policing, content moderation, and the tracking and reporting of suspicious behaviour. Predictive policing uses AI algorithms to analyse vast datasets, identifying potential criminal activities threats. For instance, police departments in the United States (US) implemented AI systems that predicted potential crime hotspots, reporting a reduction in crime rates (Brayne, 2020). Similarly, a collaborative effort in the UK and the US has led to AI being employed to forecast potential human trafficking incidents, enabling preemptive action (Furlong, 2023).

Content moderation techniques, which can include both AI and manual review, have been instrumental in detecting and removing online content related to human trafficking (Montasari & Jahankhani, 2021). However, they have also been subject to numerous critiques, including lack of resources—especially in non-English languages, gender bias, and overenthusiastic censorship. The practice of shadow banning, for example, which reduces the number of people that see a certain social media post without alerting the account holder, has been accused of unfairly targeted women human rights defenders and transgender people, reducing their ability to reach their audience (Leerssen, 2023). As explained by Savolainen (2022), however, the practice, including its methodology, is not acknowledged by social media companies, making empirical research in this domain quite difficult.

Moreover, AI has been piloted as chatbots, offering tools and advice for victims of trafficking. For example, the development of chatbots and AI-driven platforms provides victims with discreet means of seeking help and reporting their situations without alerting those responsible for the violence—often spouses (Quinn, 2019). These AI applications can also be used to analyse migration patterns and smuggling routes, offering insights into trafficking networks (Sassetti & Thinyane, 2023).

To a lesser extent, there have been efforts to use AI to safeguard women's virtual identities to protect women from virtual exploitation. This is particularly the case in the growing use of AI tools for content monitoring of social media platforms, notably following a reported increase in online misogyny and hate speech during the COVID-19 pandemic (Huertas-Garcia et al, 2023). Several governmental and regional organisations also report using AI to find evidence of the virtual exploitation of children (RESPECT International, 2019). Rodriguez et al (2021) document three categories of AI tools relevant to combatting virtual exploitation: online detection (of cases of grooming, sexual exploitation, and calls for help); safety (apps or devices where women can share their location, call for help, or report a crime); and education (where girls and women can more easily identify virtual risk factors and protect themselves from them).

3.1.3 AI as the target: Gender risks in the exploitation of AI systems

Finally, it is important to consider AI not only as a tool but also, increasingly, as a target of SOC activities. This new SOC field not only emphasises the need to secure AI technologies but also raises concerns about the exploitation of existing gender risks within these systems. AI algorithm poisoning, hacking of AI systems to steal personally identifiable information (PII) or stalk women, and sabotage of AI safety systems or biometrics represent significant threats (Wachter et al., 2017).

Although gender-related crimes targeting AI have not yet been documented, they are becoming increasingly possible. AI algorithm poisoning, for example, could potentially insert gender bias into systems used for job application screenings, financial tools, or healthcare diagnostics. This deliberate manipulation would exacerbate gender biases, locking women and gender-diverse individuals out of opportunities or exposing them to biased healthcare outcomes.

Similarly, the hacking of AI systems to steal PII or facilitate stalking women underscores the gendered nature of cyber threats, where women often face disproportionate risks of cyberstalking and online harassment (Wachter et al., 2017). There have been many recent incidents involving hacking generative AI tools—either in order to unearth vulnerabilities that could later be addressed, or as outright data theft. The most important vulnerability in generative AI tools that use prompts is now called 'prompt-injection attacks', in which hackers craft specific prompts designed to spit out PII (Burgess, 2023b).

Box 2: An intersectional approach to AI, gender, and SOC

An intersectional approach to understanding the risks associated with AI in the context of SOC emphasises the layered vulnerabilities of historically or currently marginalised groups. These risks are prevalent both when AI is utilised within SOC activities and when employed to counteract these crimes. The implications of AI in SOC are influenced by intersecting factors, each contributing to a nuanced understanding of AI's societal impact.

Race and/or Skin Colour: Discriminatory biases in AI algorithms can exacerbate racial profiling and injustices, particularly in surveillance and predictive policing. An example of this is the misidentification rates of facial recognition technology, which have been found to be significantly higher for women of colour, leading to false accusations and arrests (Buolamwini & Gebru, 2018).

Age: Younger and older populations may face distinct vulnerabilities online, including targeted scams or digital manipulation. Elderly individuals, for instance, have been disproportionately targeted by AI-driven financial scams, exploiting their lesser familiarity with digital environments (Zhang et al, 2023).

Gender Expression: AI systems can reinforce harmful stereotypes and biases, affecting gender-diverse individuals in digital spaces. For example, gender recognition software often misgenders trans and non-binary individuals, contributing to a sense of exclusion and discrimination (Keyes, 2018).

Language: Non-dominant language speakers may encounter barriers to accessing AI-driven services or protections. For example, voice-recognition systems have shown lower accuracy rates for speakers of dialects or accents that deviate from the training data's norm, limiting access to AI benefits (Hagerty & Rubinov, 2019).

Culture: Cultural contexts influence the impact of AI on privacy, consent, and digital security. In societies with collective cultural norms, the widespread use of AI in surveillance technologies can be particularly intrusive, affecting community trust and cohesion (Hagerty et al, 2019).

Digital Literacy: Varying levels of digital literacy can affect individuals' ability to navigate, respond to, or protect themselves from AI-enabled SOC threats. Those with lower digital literacy are more susceptible to misinformation and manipulation by AI-driven content (Li et al, 2024).

Digital Access: Disparities in digital access can lead to unequal exposure to or protection from AI-related risks in SOC. Rural communities, for example, often have limited access to high-speed internet and AI-driven educational or safety tools, increasing their vulnerability to digital crimes (Van Dijk, 2020).

Adopting an intersectional lens in the development of AI technologies and policies is crucial in ensuring that AI solutions do not inadvertently exacerbate existing inequalities or introduce new forms of discrimination.

3.2 Effects of New AI Advances on Gender and SOC

There are many potential and realised effects of the dynamics described above. In the section below, we provide a deeper look at the impact of AI advances on policing, on the role of women inside SOC organisations, and on transnational crime.

3.2.1 AI increasing women's vulnerability to crime

The financial difficulties and exploitation that often characterise the risk factors for joining SOC (Europol, 2021) or for being victimised are exacerbated for women and girls when AI-driven systems discriminate or stereotype based on gender. Gender risks associated with AI—including discrimination, stereotyping, and exclusion (Noble, 2018; Buolamwini & Gebru, 2018)—pose significant threats by potentially heightening the vulnerabilities that predispose women and girls to criminal exploitation and victimisation. For instance, AI technologies used in hiring, lending, and law enforcement can perpetuate gender biases, limiting economic opportunities and increasing encounters with law enforcement based on biased data (Eubanks, 2018; Keyes, 2018).

Estimates show that women would be considerably more at risk than men from labour displacement due to AI. A 2023 study from the International Labour Organization finds that although more jobs globally may be augmented by AI than completely replaced, women are the ones who will disproportionately be affected by automation (International Labour Organization, 2023). This is due in large part to the likely automation of many clerical positions more often held by women, such as secretaries, accountants, and administrators.

These systemic biases and future effects will not only impact the socioeconomic status of women and girls but also place them at a higher risk of being targeted by SOC networks, both as victims and as perpetrators. Addressing AI-driven gender stereotypes requires a concerted effort to incorporate gender-aware data and algorithms in the development and deployment of AI systems, while addressing job losses requires efforts to ensure that there are alternatives in place for women in the labour force.

Box 3: Connecting AI, cybercrime, and transnational crime

AI-combatted or AI-enabled SOC overlap with cybercrime; however, AI can enable or combat both cybercrime and non-virtual crimes. By nature, cybercrime is transnational (UNODC, n.d.), and therefore any AI criminality that is part of cybercrime can be considered transnational as well.

AI is particularly useful in combatting transnational crime, because it allows for complex patterns to emerge, such as trafficking routes, drug production supply chains, and evidence of money laundering. However, AI can also be used to combat local crime, and, as we have seen, is increasingly used in policing.

Recent discussions and studies have highlighted various ways in which AI technologies are being utilised or could potentially be exploited for transnational crimes. A comprehensive study published in *Crime Science* identified a wide range of AI-enabled future crimes, rating them based on harm, criminal profit, achievability, and defeatability. Although the study does not specifically categorise crimes as transnational, the nature of AI-enabled crimes inherently crosses borders due to the global accessibility of digital platforms and networks. For instance, AI can facilitate sophisticated cyber-exploitation, including non-consensual pornography and deepfake content creation, posing significant challenges to individual privacy and security on a global scale (Caldwell et al, 2020).

3.2.2 The nuanced impact of AI, gender, and SOC on policing

There has been significant enthusiasm in integrating AI into law enforcement operations in the last few years, from the potential of improved data analysis, predictive policing, and automation, potentially leading to more efficient crime detection and prevention (Ferguson, 2017). In fact, AI is already being integrated into the activities of police forces around the world.

The metropolitan police of many large cities, for example London and New York, include complex data fusion systems which combine various surveillance methodologies and can flag potential criminal activity, whether real or simply possible (Carnegie Council for Ethics in International Affairs, 2024). Many jurisdictions use body cameras on police officers, which collect data that AI tools can later analyse. Biometric surveillance is being used increasingly in large cities or during large gatherings, such as football matches, especially in relation to crime anticipation (Castets-Renard, 2021). AI is not only used in metropolitan policing and in the detection of criminal individuals but also in larger investigative operations, either at national levels (such as the Royal Canadian Mounted Police in Canada) or at international levels (such as Europol in Europe), which have adopted AI tools to track more complex criminal operations. Police are also implementing predictive policing, detecting areas and times for potential criminal activity and increasing police activity in response.

Benjamin (2019), Buolamwini and Gebru (2018), and Noble (2018) were early to note the impact of race and gender on policing using AI. They documented how facial recognition systems commonly used by police to identify criminals were particularly prone to error for women and people of colour, with the worst errors involving women of colour; for example, in 2024, a woman was arrested wrongfully in Detroit for a carjacking (Hill, 2023). This issue has also been documented by the Carnegie Council on Ethics in International Affairs, which noted the use of data fusion tools in policing marginalised groups (2024). However, visibility on this issue may have led to some improvements. In the UK, a 2023 audit of police facial recognition systems conducted by the National Physical Laboratory concluded that if AI systems were configured properly, the demographic errors could be reduced significantly (Mansfield, 2023). UK-based Big Brother Watch therefore recently suggested that AI tools be used to fight serious crime, but not for minor crimes (Gikay, 2023).

3.2.3 AI and the changing roles of women in SOC

The traditional narrative surrounding the role of women in SOC has often relegated them to peripheral roles; however, recent evidence suggests that women's participation as perpetrators within SOC is on the rise. This shift not only challenges the conventional gender stereotypes associated with criminal activity but also indicates a complex evolution in the dynamics of SOC (Allum & Gilmour, 2019; Fiandaca, 2007). The increasing involvement of women in SOC underscores the need for a nuanced understanding of gender roles within these illicit networks.

For instance, exploitation of AI biases could lead to scenarios where female criminals exploit security systems’ inability to recognise them as threats. Moreover, AI’s role in enhancing security and anonymity can provide women in SOC with new tools for evading detection, particularly in areas like cyber fraud. The increased autonomy for women in SOC, especially in the fraud sector, highlights the double-edged nature of AI in criminal activities, where technological advancements can also increase criminal opportunities.

There is evidence that digital tools have allowed women to become more independent and empowered in certain fields (Sadrul et al, 2023), allowing them to succeed outside of traditional structures, both legal and illegal. Historically, SOC has tended to operate as entities, such as mafias and gangs, which have mimicked male-dominated structures in the legal economy. While women were present in all aspects of these crime organisations, they were much less represented than men, with some estimates of about 10 per cent of female participation throughout, and much lower for participation in leadership.

However, women are using digital tools to increase their economic independence, as they are typically more likely to lead small enterprises than large ones, for a variety of factors. Examples include the rise of the female influencer on social media—a path for economic independence for many women—and the increase in women-led e-commerce businesses. Similarly, we see many women-led initiatives in the AI sector, such as Connected Women, an organisation in the Philippines which trains women in AI skills and employs them in outsourcing contracts with large AI companies (Connected Women, n.d.). It is possible, therefore, that women’s participation in SOC as offenders could be enabled by AI, given parallel changes in women’s engagement in other economic sectors. Since 2022, there has been a notable development and adaptation of generative AI tools tailored for malicious use. These tools, which can autonomously generate phishing emails, fake websites, and other deceptive digital content, are readily available for download and can be operated independently by criminals, including women who are increasingly participating in these sectors (Landi, 2023).

Moreover, the digital transformation of crime networks has led to more flexible and anonymous online operations, traits that potentially make SOC more accessible and appealing to women. The anonymity offered by the digital domain lowers the barriers to entry and diminishes the risk of detection, particularly for those involved in sophisticated schemes such as human trafficking and recruitment into violent extremism and terrorism. This shift underscores the increasing importance of digital skills within SOC, where proficiency in AI and cyber technologies is becoming a critical asset. The use of AI for training and recruitment into SOC highlights a worrying trend where technology not only facilitates traditional crimes but also breeds new forms of criminal activities that are more elusive and challenging to combat (INTERPOL & UNICRI, 2020).

It is, however, possible to examine the list of individual risk factors for participation in SOC to examine why women have a lower participation rate in SOC, and whether AI would impact that. Table 2 lists certain risk factors outlined by the UK Government's Help Desk Report on Gender and Serious and Organised Crime, highlighting where AI could have a particular affect on women (United Kingdom Government, n.d.; Enfield, 2019).

Table 2: Impact of AI on the risks of being drawn into SOC

Factor	Dimensions	Effect of AI on Women
Networks	Online	The changing nature of online networks may affect the exposure of women to SOC, potentially making them more exposed than in the past.
Ability	Criminal Skills	AI skills are now considered part of the criminal skills toolkit and could potentially mean higher participation if women's representation in AI increases.
	Criminal Access	Access to criminal opportunities has changed, with transnational and virtual crime on the rise. For women, physical presence in the location of the crime may no longer be necessary.
Identity	Pro-Criminal Attitudes	Women may be exposed online to pro-criminal attitudes and may even participate in their creation. These attitudes could increasingly be disseminated through AI.
	Financial Difficulties	Important changes in the labour force due to AI threaten to displace many workers, with an emphasis on certain jobs held by women. This, coupled with AI-driven discrimination, could increase the economic vulnerability of women.
	Victim of Exploitation	AI-enabled exploitation that affects women includes trafficking, identity theft, and impersonation.

3.3 Future Gender Risks of AI and SOC

A key finding of this study is that data collection about women and SOC may be threatened by the increased digitisation of the field, unless gender data is explicitly collected. As more activities take place online, anonymity online means less data on women's involvement. Notably, this online anonymity is seen in the increase in adoption of End to End Encryption, which can mean less detection of all criminals, including women. As explained by Enfield (2019): "*Technology has created a range of new opportunities for criminals. […] The sharing of indecent images of children, for example, is now almost entirely enabled by the internet. However, gender distinctions between victims, consumers and purveyors of images are unrecorded.*"

In addition, as new AI developments are released, there are considerable concerns about misuse—not only of the tool itself but also of the source code. Many AI tools are released with publicly accessible models, which means that these models can be repackaged for harmful use. Malicious generative AI tools, for example, such as Worm GPT, FraudGPT, XXXGPT, have all been built to harness the new technologies for SOC (Infosecurity Europe, 2023). This means that any risk outlined in this report can be further accentuated by new technological releases that allow reuse—a core philosophical tenet of foundational models.

Finally, increased digitisation more generally raises important concerns about privacy, cybersecurity, and surveillance. As we have seen, women and girls are particularly vulnerable to breaches in online data and property, which can lead to physical or virtual assault, or other crimes such as fraud and blackmail. In this sense the acceleration of AI adoption across various sectors is also hastening digital transformation more broadly, where privacy and cybersecurity concerns are increasing.

Box 4: The impact of data gaps in understanding AI, gender, and SOC: Illegal drugs

There are many examples of serious gaps in data which reduce the impact of a gender lens. One gap is in the way in which gender plays a factor on the impact of AI on illegal drugs.

Human beings can be victimised by the illegal drug trade regardless of gender. According to the US-based National Institute on Drug Abuse (n.d.), men are more likely to abuse illegal drugs, although both women and men are equally susceptible to addiction. AI-based tools have been used to enable and combat illegal drugs and are beginning to be instrumental in disrupting drug networks (Caldwell et al, 2020).

For example, the European Commission has launched a fund to support research into the use of AI to discover illegal drug production and trafficking (European Commission, 2023). The South Korean Ministry of Food and Drug Safety has also launched a project to use AI to fight illegal drug distribution (Da-hyun, 2024). On the Venezuela and Columbia border, geospatial intelligence and AI have been used to locate potential coca paste production (Hidalgo & Centeno, 2023). An AI-based tool was also used by the US border patrol to map the supply chain in the different ingredients required for fentanyl assembly, allowing agents to track billions of transactions (Axios, 2023). In 2024, the US government announced that it would hire 50 AI experts to address drug trafficking and child abuse (Reuters, 2024).

AI-based tools have been used quite differently to enable drug trafficking; notably, in the use of AI-based social media recommendation systems and generative AI tools, which have allowed for the creation and dissemination of illicit drug advertisements to potential buyers.

>> There has not yet been a study of whether these drug trafficking detection tools might apprehend or protect women in different ways than men.

>> It is unknown whether or not the reach of recommendation systems on social media have a gender dimension when it comes to drugs.

3.4 Regulatory Initiatives Addressing AI, Gender, and SOC

Recent advances in national and global AI regulation, spanning from 2022 to 2024, have significantly impacted the landscape of SOC, introducing new frameworks for addressing gender-related issues within this context. The European Union's AI Act has passed its last major hurdle towards adoption, aiming to regulate applications of AI based on a risk-based approach. This AI Act delineates prohibitions on specific uses of AI, governance rules for high-risk applications, and transparency requirements for AI systems, excluding low-risk applications from its scope. This approach is expected to set a global standard for AI usage across various sectors, including those related to SOC (European Parliament, 2023).

In addition to the European Union's AI Act, there are many other regulatory initiatives in progress, from the UK's 2023 Safety Summit to the US's 2023 Executive Order on AI. The UN has led a number of global governance initiatives on AI, including UNESCO's Recommendations on the Ethics of AI (2021b) and the work of the AI Advisory Body, due for completion before the Summit of the Future in 2024. In 2023, UN Women and the Commission on the Status of Women (CSW) focused on technology and gender, with several components of the 2024 CSW on AI, and a possible further focus on AI at the 2025 CSW.

In the UK and globally, there have been increasing efforts to protect victims of AI-enabled abuse. Notable in this domain is the Online Safety Act, adopted in October 2023, which requires platforms to go much further in protecting users, including eliminating child pornography, criminalising AI-generated intimate images, and better protecting privacy.

There have been calls to better link existing instruments on organised crime and gender—notably the Palermo Protocols (officially the United Nations Convention against Transnational Crime), the WPS Agenda, and the Convention on the Elimination of all Forms of Discrimination Against Women—to ongoing AI and digital platform regulatory efforts (Zinser, & Thinyane, 2021; Coombs & Abraha, 2023).

4. Mitigation Approaches and Recommendations

Given the complex interplay of AI, gender, and SOC, this report makes recommendations in two categories: policy, which could be adopted in municipal, national, and global jurisdictions; and technical, which could be addressed by AI companies.

Policy Recommendations

1. WPS and SOC policy forums share common concerns over AI and women's safety. It would be relevant to use future opportunities, such as the CSW, to initiate a common effort to add to the global governance instruments in each case; for example, the WPS Agenda and the Palermo Protocols.

2. Ongoing national and global AI governance processes should mainstream gender considerations, which could include the collection of gender-based data for all AI risks and opportunities.

3. National governments should ensure that AI used in policing is properly audited and regularly revisited, with different strategies used for day-to-day policing of minor offences versus larger transnational efforts.

4. National governments should prioritise investing in responsible AI tools to combat gender-based criminal victimisation, especially to understand the phenomenon and address it in policy.

Technical Recommendations

1. Generative AI companies should prioritise eliminating stereotyping and discrimination in their tools, which can have significant effects on the systemic vulnerability of women, notably by conducting gender impact assessments *before* deployment.

2. Technical standards used by AI companies, such as the US-based National Institute of Standards and Technology standards, should include gender and SOC impact assessments that all public-facing tools should conduct before deployment.

3. All AI companies, with a focus on generative AI companies and social media platforms, should further prioritise reducing misuse of their tools, by developing much better guardrails for women's protection before the tools are deployed, especially in non-English languages and varied cultural contexts.

Overall, the mitigation of gender risks in AI and SOC will require a layered approach, with government, multilateral organisations, and AI companies working together to address the many issues highlighted in this report. Additionally, as new AI technologies are released, it will be important to consider not only their serious potential negative impact on gender and SOC but also their opportunities in combatting crime, if they are deployed responsibly.

Annex: References

Aiken, M. (2016). *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*. Spiegel & Grau.

Albrecht, E., Fournier-Tombs, E., Brubaker, R. (2024). Disinformation and Peacebuilding in Subsaharan Africa. UNU Research Report. Retrieved from https://collections.unu.edu/eserv/UNU:9419/disinformation_peacebuilding_subsaharan_africa.pdf

Allum, F., & Gilmour, S. (Eds.). (2019). *The Routledge Handbook of Transnational Organised Crime*. Routledge.

Aronowitz, A., & Chmaitilly, M. (2020). Human Trafficking: Women, Children, and Victim-Offender Overlap. Oxford Research Encyclopaedia of Criminology. Retrieved from https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-609.

Axios. (2023). Customs and Border Protection is using AI to crack down on fentanyl trafficking. Retrieved from https://www.axios.com/2023/12/07/fentanyl-trafficking-ai-border-patrol

Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press.

Brayne, S. (2020). *Predict and Surveil: Data, discretion, and the future of policing*. Oxford University Press.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91). PMLR.

Burgess, M. (2023). Deepfake Porn is Out of Control. Wired. Retrieved from https://www.wired.com/story/deepfake-porn-is-out-of-control/

Burgess, M. (2023b). The Security Hole at the Heart of ChatGPT and Bing. Wired. Retrieved from https://www.wired.co.uk/article/chatgpt-prompt-injection-attack-security

Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. *Crime Sci* **9**, 14 (2020). https://doi.org/10.1186/s40163-020-00123-8

Carnegie Council for Ethics in International Affairs (2024). Carnegie Council Launches Tool Mapping the Impact of Data Fusion Technology on Freedom, Security, and Human Rights. Retrieved from https://www.carnegiecouncil.org/about/news/press-release/carnegie-council-launches-tool-mapping-the-impact-of-data-fusion-technology-on-freedom-security-and-human-rights

Castets-Renard, C. (2021). *Human Rights and Algorithmic Impact Assessment for Predictive Policing*. *Constitutional Challenges in the Algorithmic Society*. Cambridge University Press, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3890283

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.*, *107*, 1753.

Cho, B., Le, B. M., Kim, J., Woo, S., Tariq, S., Abuadbba, A., & Moore, K. (2023, October). Towards understanding of deepfake videos in the wild. In *Proceedings of the 32nd ACM International Conference on Information and Knowledge Management* (pp. 4530-4537).

Connected Women (n.d.) Website retrieved from https://connectedwomen.com/

Coombs, E., & Abraha, H. H. (2023). Governance of AI and gender: Building on International Human Rights Law and relevant regional frameworks. In *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (pp. 211-243). Edward Elgar Publishing.

Da-hyun, J. (2024). AI monitoring systems target illegal drug sales online. The Korea Times. Retrieved from https://www.koreatimes.co.kr/www/nation/2024/03/113_366822.html

Dodd, V & Milmo D. (2023). AI could worsen epidemic of child sexual abuse, warns UK Crime Agency. The Guardian. Retrieved from https://www.theguardian.com/society/2023/jul/18/ai-could-worsen-epidemic-of-child-sexual-abuse-warns-uk-agency

Dunn, S., Vaillancourt, T., & Brittain, H. (2023). Supporting Safer Digital Spaces. Centre for International Governance Innovation.

Dymples, S. (2022) Deepfakes and Disinformation in Southeast Asia. In Filimowicz, M. (Ed.). (2022). *Deepfakes: Algorithms and Society* (Ser. Algorithms and society). Routledge.

Enfield, S. (2019). Gender and Serious and Organised Crime. Helpdesk Report. Retrieved from: https://assets.publishing.service.gov.uk/media/5cb84ce640f0b649df5bf9f5/561_Gender_and_Serious_and_Organised_Crime.pdf

Eubanks, V. (2018). Automating Inequality. St. Martin's Press.

European Commission. (2023). ARtificial IntelligencE in fighting illicit drugs production and trafficking. Horizon Europe. Retrieved from https://cordis.europa.eu/project/id/101121329

European Institute for Gender Equality. (2017). Cyberviolence is a growing threat, especially for women and girls. Retrieved from https://eige.europa.eu/newsroom/news/cyber-violence-growing-threat-especially-women-and-girls?language_content_entity=en

European Parliament (2023). EU AI Act: first regulation on artificial intelligence. Retrieved from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Europol. (2021). New report finds that criminals leverage AI for malicious use – and it's not just deep fakes. Europol. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-%E2%80%93-and-it%E2%80%99s-not-just-deep-fakes

EY (2023). Using AI to Combat Money Laundering. Retrieved from: https://www.ey.com/en_us/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

Fiandaca, G. (Ed.). (2007). *Women and the Mafia: Female Roles in Organised Crime Structures*. Springer.

Fournier-Tombs, E., & Castets-Renard, C. (2021). Algorithms and the Propagation of Gendered Cultural Norms. Forthcoming for publication in French in 'IA, Culture et Médias' (2024). Edited by Véronique Guèvremont and Colette Brin. Presses de l'université de Laval. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3980113

Fournier-Tombs, E. (2023). A women's rights perspective on safe artificial intelligence inside the United Nations. In *Handbook of Critical Studies of Artificial Intelligence* (pp. 481-492). Edward Elgar Publishing.

Fournier-Tombs, E. (2023b). *Gender Reboot*. London: Palgrave MacMillan.

Furlong, N. (2023). *Using analytics and AI to combat human trafficking.* Open Access Government. Retrieved from: https://www.openaccessgovernment.org/analytics-ai-tackle-global-human-trafficking/157377/

Gavin, S. M., & Kruis, N. E. (2022). The influence of media violence on intimate partner violence perpetration: An examination of inmates' domestic violence convictions and self-reported perpetration. *Gender issues*, *39*(2), 177-197.

Gikay, A.A. (2023). Facial recognition helps fight serious crime, but for minor UK offences it should be off limits. The Guardian. Retrieved from https://www.theguardian.com/commentisfree/2023/dec/24/facial-recognition-uk-drivers-licence-police-lineup

GIWPS. (2020). Women in Organised Crime. Georgetown Institute for Women, Peace and Security. https://giwps.georgetown.edu

Hagerty, A., & Rubinov, I. (2019). Global AI ethics: a review of the social impacts and ethical implications of artificial intelligence. *arXiv preprint arXiv:1907.07892*.

Hill, K. (2023). Eight Months Pregnant and Arrested After False Facial Recognition Match. The New York Times. Retrieved from https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html

Huertas-García, Á., Martín, A., Huertas-Tato, J., & Camacho, D. (2023). Countering malicious content moderation evasion in online social networks: Simulation and detection of word camouflage. *Applied Soft Computing*, *145*, 110552.

InfoSecurity Europe (2023). The Dark Side of Generative AI: Five Malicious LLMs Found on the Dark Web. Retrieved from https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/generative-ai-dark-web-bots.html

International Justice Mission (2023). Scale of Harm: Estimating the Prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines. Retrieved from https://www.ijm.org/studies/scale-of-harm-estimating-the-prevalence-of-trafficking-to-produce-child-sexual-exploitation-material-in-the-philippines

International Labour Organization (2023). Generative AI and Jobs: A global analysis of potential effects on job quantity and quality. Retrieved from https://www.ilo.org/global/publications/working-papers/WCMS_890761/lang--en/index.htm

Internet Watch Foundation (2023). How AI is being abused to create child sexual abuse imagery. Retrieved from https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

INTERPOL & UNICRI. (2020). Artificial Intelligence and Robotics for Law Enforcement. Retrieved from: https://unicri.it/sites/default/files/2019-10/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB_0.pdf

Keyes, O. (2018). The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1–22.

Kotarska, G. (2023). The Importance of Gender Analysis for Understanding Organised Crime. RUSI. Retrieved from https://rusi.org/explore-our-research/publications/commentary/importance-gender-analysis-understanding-organised-crime

Landi, M. (2023). Generative AI 'helping criminals conduct more sophisticated cyber attacks'. The Independent. Retrieved from https://www.independent.co.uk/news/uk/national-cyber-security-centre-github-b2455871.html

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, 48, 105790.

Li, P., Li, Q., & Du, S. (2024). Does digital literacy help residents avoid becoming victims of frauds? Empirical evidence based on a survey of residents in six provinces of east China. *International Review of Economics & Finance*.

Lofkin, N (2023). #Cutoffthecatfish – Raising awareness of revenge porn with the revenge porn hotline. Retrieved from https://swgfl.org.uk/magazine/cutoffthecatfish-raising-awareness-of-sextortion-with-the-revenge-porn-helpline/

Luengo-Oroz, M., Bullock, J., Pham, K. H., Lam, C. S. N., & Luccioni, A. (2021). From artificial intelligence bias to inequality in the time of COVID-19. *IEEE Technology and Society Magazine*, *40*(1), 71-79.

Mansfield, T. (2023). Facial recognition technology in law enforcement equitability study. National Physical Laboratory. Retrieved from https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

McAfee (2024). Love Bytes: How AI is Shaping Modern Love. Retrieved from https://www.mcafee.com/blogs/internet-security/love-bytes-how-ai-is-shaping-modern-love/

Montasari, R., & Jahankhani, H. (2021). The Application of Technology in Combating Human Trafficking. In *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021* (pp. 149-156). Cham: Springer International Publishing.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

OECD. (2023). OECD AI Principles Overview. Retrieved from https://oecd.ai/en/ai-principles

OSCE. (2023). Understanding the role of women in organised crime. Retrieved from https://www.osce.org/files/f/documents/0/4/560049.pdf

Parti, K., Dearden, T. E., & Hawdon, J. (2022). Understanding the overlap of online offending and victimization: Using cluster analysis to examine group differences. *Victims & Offenders*, *17*(5), 712-734.

Pinto Hidalgo, J. J., & Silva Centeno, J. A. (2022). Geospatial intelligence and artificial intelligence for detecting potential coca paste production infrastructure in the border region of Venezuela and Colombia. *Journal of Applied Security Research*, *18*(4), 1000-1050.

Quinn, C (2019). Using AI in accessing justice for survivors of violence. UN Women Asia and the Pacific. Retrieved from https://asiapacific.unwomen.org/en/news-and-events/stories/2019/05/using-ai-in-accessing-justice-for-survivors-of-violence

Raets, S., & Janssens, J. (2021). Trafficking and technology: Exploring the role of digital communication technologies in the Belgian human trafficking business. *European journal on criminal policy and research*, 27, 215-238.

RESPECT International (2019). Artificial Intelligence Combatting the Online Sexual Abuse of Children. Retrieved from https://respect.international/wp-content/uploads/2019/11/AI-Combating-online-sexual-abuse-of-children-Bracket-Foundation-2019.pdf

Reuters. (2024, February 2). Europe within reach of landmark AI rules after nod from EU countries.

Rodríguez, D. A., Díaz-Ramírez, A., Miranda-Vega, J. E., Trujillo, L., & Mejia-Alvarez, P. (2021). A systematic review of computer science solutions for addressing violence against women and children. *IEEE Access*, *9*, 114622-114639.

Rosenblat, A., & Stark, L. (2016). Algorithmic labor and information asymmetries: A case study of Uber's drivers. *International Journal of Communication*, 10, 3758-3784.

Sadrul Huda, S. S. M., Akter, S., & Safder, A. (2023). Technology enabled entrepreneurship: Ekshop and rural women in Bangladesh. *Journal of Information Technology Teaching Cases*, 20438869231203339.

Sarkar, S. (2015). Use of technology in human trafficking networks and sexual exploitation: A cross-sectional multi-country study. *Transnational Social Review*, *5*(1), 55-68.

Sassetti, F. & Thinyane, H. (2023) Apprise: Inclusive innovation for enhancing the agency of vulnerable populations in the context of anti-trafficking responses. *Innovation and Development*, 13:1, 173-191, DOI: 10.1080/2157930X.2020.1854249

Savolainen, L. (2022). The shadow banning controversy: Perceived governance and algorithmic folklore. *Media, Culture & Society*, *44*(6), 1091-1109. https://doi-org.proxy3.library.mcgill.ca/10.1177/01634437221077174

Stop the Traffik. (n.d.). Definition and Scale. Retrieved from https://www.stopthetraffik.org/what-is-human-trafficking/definition-and-scale/

Strengers, Y. & Kennedy, J. (2021) *The Smart Wife*. Boston: The MIT Press.

TrendMicro. (2021). Gender in Cybercrime. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gender-in-cybercrime

UNESCO (2021). The chilling: Global trends in online violence against women journalists. Research discussion paper. Retrieved from https://unesdoc.unesco.org/ark:/48223/pf0000377223

UNESCO (2021b). Recommendations on the Ethics of AI. Retrieved from https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

United Kingdom Government. (n.d.) Serious and organised crime strategy. Retrieved from https://www.gov.uk/government/collections/serious-and-organised-crime-strategy

United Kingdom Government. (2023). International development in a contested world: Ending extreme poverty and tackling climate change. A white paper on international development. Retrieved from https://assets.publishing.service.gov.uk/media/6576f37e48d7b7001357ca5b/international-development-in-a-contested-world-ending-extreme-poverty-and-tackling-climate-change.pdf

United Kingdom Government (2024). AI Scams: Consumer Protection. Hansard Volume 744. Retrieved from: https://hansard.parliament.uk/commons/2024-01-22/debates/7D5CB585-963A-426A-9168-3A222F27A821/AIScamsConsumerProtection

United Nations Office on Drugs and Crime (UNODC). (n.d.). Organised Crime Module 15 Key Issues: Gender and organised crime. UNODC. Retrieved from https://www.unodc.org/e4j/en/organised-crime/module-15/key-issues/gender-and-organised-crime.html

United Nations Office on Drugs and Crime (UNODC). (2020). Mainstreaming gender in organised crime and illicit activity projects. Retrieved from https://www.unodc.org/documents/Gender/Thematic_Gender_Briefs_English/Org_crime_and_trafficking_brief_23_03_2020.pdf

United Nations Office on Drugs and Crime (UNODC). (2022). Global Report on Trafficking in Persons. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2022/GLOTiP_2022_web.pdf

University College London. (2020, August 4). 'Deepfakes' ranked as most serious AI crime threat. UCL News. https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

UN Women. (2024, Forthcoming). AI and the Women, Peace and Security Agenda in Southeast Asia.

UN Women. (2023). Creating safe digital spaces free of trolls, doxing and hate speech. Retrieved from https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech

UN Women. (n.d.) Concepts and definitions. Retrieved from https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm

Van Dijk, J. (2020). *The Digital Divide*. John Wiley & Sons.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6).

West, S. M., Whittaker, M., & Crawford, K. (2019). Discriminating systems: Gender, race, and power in AI. AI Now Institute.

Zhang, T., Morris, N. P., McNiel, D. E., & Binder, R. (2023). Elder Financial Exploitation in the Digital Age. *The Journal of the American Academy of Psychiatry and the Law*, JAAPL-220047.

Zinser, S., & Thinyane, H. (2021). A Step Forward for Palermo's Trafficking Protocol, This Time Integrating Frontier Technology. *Yale J. Int'l Aff.*, *16*, 140.

Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist — it's time to make it fair. *Nature*, 559, 324-326