EUROPOL

Intelligence Notification

Trafficking in human beings and the internet

Rapid innovations in information and communication technologies facilitate the trafficking in human beings (THB) by exposing a growing number of victims to traffickers. These traffickers use social networks and online classified sites to market, recruit, sell and exploit their victims.

The internet has shifted the recruitment, advertising and selling process from the street to the digital domain. Online interaction creates both risks and opportunities for criminals, victims and law enforcement. Criminals and victims leave permanent traces, which facilitates identification, but not necessarily intervention. This gap between identification and intervention is becoming more difficult to overcome for law enforcement. This issue is also covered in Europol's Serious and Organised Crime Threat Assessment (SOCTA) 2013.

This Intelligence Notification provides an overview of Europol's knowledge on the role of the internet as a facilitator for THB.

Key trends

- A shift to the virtual space affects many activities related to THB. Certain types of sexual exploitation take place online entirely such as live videos or sex chats. In other cases, exploitation is heavily facilitated by websites that aid setting up encounters with customers.

- New *modi operandi* have emerged in the context of exploitation such as the digital surveillance or blackmailing of victims. These activities on their own may constitute crimes.

- Traffickers use both specialised exclusive online platforms (escort websites) and general advertising platforms to attract customers.

- The use of internet platforms allows OCGs to exploit victims of sex trafficking on a much larger scale. Traffickers advertise their victims in extensive online catalogues. OCGs are able to manage dozens of victims at the same time. The OCGs involved are highly organised and mobile, operating across numerous countries and jurisdictions. They operate both independently and in collaboration with other crime groups. Collaboration with other groups is typically based on the need to procure specialised services offered by other OCGs.

- In the context of child sexual exploitation, social media outlets allow perpetrators easier access to potential victims and greatly facilitate their recruitment. The internet enables perpetrators to anonymously share child abusive material and exchange information on specialised forums such as experience and recommendations regarding favourite destinations for child abuse and ways to handle encounters with local police.

The internet as a facilitator for trafficking in human beings

The internet is a key facilitator for THB with an impact on the entire trafficking chain from recruitment and transportation to the harbouring of the victims and their actual exploitation.[1]

The recruitment of victims increasingly takes place online. Traffickers lure victims with promising advertisements for jobs or travel placed on general advertisement sites or distributed through au pair agencies, international marriage agencies or dating sites. In addition to adverts, traffickers also directly approach victims in chat rooms or on mainstream social media.

1

Intelligence Notification

The adverts placed to recruit victims of sexual exploitation typically offer work in administration, cleaning or child care. Victims targeted for labour exploitation are attracted by online advertisements promising employment in agriculture, collecting and delivering charity bags, construction, the cleaning or transportation sectors.

The internet also facilitates the transportation of victims. Traffickers often purchase tickets online using compromised credit card data in order to hide their identities. By using stolen credit card information, neither the tickets nor the victims can be easily linked back to the facilitators/exploiters.

Online technologies also enable traffickers to more easily harbour and control victims. OCGs maintain close surveillance of their victims, by imposing daily e-mail exchanges or chat sessions to prove their presence. Victims can also be monitored using live cameras, which are often justified as security measures for their safety.

OCGs use the internet to threaten or coerce victims of THB. The internet is used to blackmail victims, by threatening to send compromising pictures to their family or friends or to expose them online. OCGs can also easily blackmail the clients of the sexual services they organise. In many cases, clients make bookings and pay online directly to the organisers, making their contact details available to OCGs.

The internet facilitates direct exploitation and creates new forms of exploitation. Whole catalogues of exploited women are placed online containing pictures and contact details. Clients can order these women directly online and are also able to pay online in some cases. Clients and victims meet at a specific location or the victim is sent to the client's location. Some victims are exploited on specialised websites offering webcams or sex chats. Victims forced to offer services on these websites are also often exploited financially by being coerced to pay additional fees to have their advertisements displayed online.

Forced activities involving webcams or sex chats fully take place online. Websites for escort services are used as a legitimate façade to offer services associated with sexual exploitation. In some cases, traffickers transport victims to the country of exploitation on orders placed through these websites.

The internet as a provider of opportunities for expansion - links to online fraud

The internet provides traffickers with opportunities to reach a broader and more diverse pool of victims and customers. The online exploitation of victims provides various revenue streams to OCGs. In addition to payments from clients, OCGs also charge their victims for advertisement costs. Some OCGs use commercial online advertising and pay using compromised payment card data obtained online.

OCGs use the internet to expand their activities internationally. OCGs often recycle the material used for specific "national" websites to develop new ones aimed at reaching customers in other targeted countries. The same materials are uploaded to different domains. Clients can either choose to visit the girls in the countries of origin or have them brought to their countries. Victims travel between different countries on demand and OCGs easily shift the location of their activities to other countries in order to avoid law enforcement attention.

The use of online services can anonymise activities, but also entails the risk of leaving traces. OCGs use various tools and techniques such as dynamic IPs, multihoming[2], pseudonyms and registering websites abroad to obscure their identities.

The internet, internet-enabled mobile devices and applications facilitate communication among OCG members as well as the transfer of money.

Opportunities for law enforcement

The internet facilitates the activities of OCGs engaging in THB. However, the internet, online technologies and large amounts of openly available data can also enhance the work of law enforcement agencies (LEAs). A combination of advanced computer-assisted data gathering and analysis techniques can detect online trafficking.

LEAs can also use the internet to raise public awareness for THB. Social media platforms are very effective tools to execute information campaigns.

Crowd-sourcing of information also has the potential to be an effective law enforcement tool. Engaging the public in the fight against THB may encourage citizens to share useful information with the police.

Intelligence Notification

Challenges for law enforcement

While online classified advertising sites remain an important focus for law enforcement, a variety of other social, informational, and mobile networking sites also play an increasingly important role in the recruitment of minors for sex trafficking. These websites act as hubs for communication between trafficker-pimps and trafficked minors.

Internet-facilitated trafficking takes place on a global scale, which complicates investigations. Effective information-sharing across multiple jurisdictions is of utmost importance for law enforcement agencies. Europol can provide vital services in facilitating the exchange of information and performing operational analysis on data gathered online, which is crucial in identifying victims and suspected traffickers.

LEAs will need to increasingly engage with partners in the private sector in order to improve investigative outcomes and preventative measures. The private sector is a crucial partner as traffickers rely on technologies and service offerings by companies to facilitate their activities. Contacts with social media companies or domain hosts will make investigations more effective. Cooperation with companies in the financial services industry open up new opportunities for law enforcement to gather evidence and intelligence on financial transactions linked to THB. Software solutions provided by the private sector in data mining, mapping or computational linguistics could be invaluable tools in detecting cases of THB online.

The shift to internet-facilitated THB requires effective legislative and investigative responses to the use of online technologies. Currently, LEAs are limited by narrow legal frameworks in their ability to carry out investigations online.

Data found online and on mobile devices can be obtained using forensic examination and used as evidence in cases. Law enforcement specialists require continuous technical training in order to keep up with OCGs' increasing use of countermeasures such as encrypted mail and encrypted mobile devices.

Conclusion

The shift of activities to the virtual realm in the contemporary world has severely affected the crime area of trafficking in human beings. OCGs have adopted new modi operandi to integrate the internet in their trafficking activities. Law enforcement authorities have been challenged to adapt to these developments. The internet provides both opportunities and threats to the criminals involved in trafficking activities, their victims and the law enforcement authorities fighting human trafficking.

3

---

[1] In accordance with the definition of trafficking in human beings as stipulated in Article 2 Directive 2011/36/EU of the European Parliament of the Council: "The recruitment, transportation, transfer, harbouring or reception of persons, including the exchange or transfer of control over those 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"

[2] The configuration of multiple network interfaces or IP addresses on a single computer. This concept is an easy solution of migration between different types of networks when travelling