

HUMAN TRAFFICKING AS CYBERCRIME

L. M. Rhodes

Leanne Maree Rhodes

Abolishion Inc. Melbourne, Australia

*Correspondence: Leanne Maree Rhodes, Abolishion

PO Box 406, Flinders Lane, Victoria, Australia, 8009

E-mail: Leanne.Rhodes@abolishion.org

Abstract

Both the surface web and the dark web are utilised by traffickers to recruit and sell victims of human trafficking. This report explores how traffickers are using social engineering and technology to perform their trade. It looks at advances in fighting cybercrime, both legal and illegal and makes recommendations towards an increase of fighting human trafficking in cyberspace.

Key Words

human trafficking, dark web, cybercrime, online child exploitation, social engineering

Introduction

Human trafficking is a heinous crime against humanity that is devastating the lives of an estimated 45.8 million people in the world today. Many understand that modern day slavery was removed from our world last century with the abolitionist efforts of William Wilberforce, Abraham Lincoln and the many that stood by their sides. However, human trafficking still lives amongst us and is growing at an alarming rate. In fact, there are more people in slavery today than at the time we thought human trafficking left us. There are various factors of evolution in the systems of our modern day society that have contributed to the growth of this blight against humanity. The rise of the internet and particularly the dark web are enabling traffickers to operate their crime with increased ease in today's world.

Human Trafficking

The United Nations defines “trafficking in Persons as the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organ.”¹

Human trafficking is a criminal activity that is often highly organised in nature, often crossing national borders and legislative reach. Traffickers operate this lucrative business, making use of the latest technology available to hide their criminal activity with little fear of being caught. The advances in technology are fast providing them with more places to hide.

¹ United Nations, Protocol to Prevent, Suppress and Punish Trafficking in Persons, 2000; Article 3, paragraph (a).

HUMAN TRAFFICKING AS CYBERCRIME

The Internet - A Platform for Human Trafficking

The rise of the internet has not only provided fast access to information for our world but has also provided faster and more efficient ways for organised crime to operate. Robert Hannigan, the Director of Communication Headquarters for the British Government stated that groups like Facebook, Twitter and WhatsApp are the “commend-and-control networks of choice for terrorists and criminals.”²

Let’s look at the example of pornography, a key industry in the human trafficking world. Fifty year ago, if someone wanted to purchase pornography they would need to go to the local criminal or corner store to buy it. Pornography was readily available however buying it had a societal stigma associated with it. The action of physically having to go and buy it would mean that someone else would know the person purchasing it, providing a natural deterrent for its demand.

In today’s world, pornography is readily available on the internet. To follow this example, if someone today was to purchase online pornography, it can be done in the privacy of their own home. No one needs to know and the natural deterrent is removed, seeing a marked increase in pornography use today.

The ease in access to pornography has also created a further market and demand for material, some of which is becoming more and more heinous in nature allowing individuals to carry out fantasies in virtual reality. The internet combined with factors such as this are providing a lucrative environment for traffickers to operate their business. Fight the New Drug claim that 25% of all search engine requests are for pornographic material³.

The Internet – A Platform for Selling

The internet is also becoming a place of choice for traffickers to sell the services they force upon their victims. One can readily access the services of escorts and prostitution online with just a few clicks using services like Backpage, Craigslist, Facebook and the many chatrooms dedicated to these services.

Online advertising is not the only method traffickers use to sell their wares but it is a key component with many traffickers ensuring online listing happens in as many places as possible. Some even force their victims to spend time online advertising themselves with both real and different photo identities. False photos are often used to hide under age exploitation.

Thorn, a NGO set up by Aston Kutcher and Demi Moore to drive tech innovation to fight child trafficking and the sexual exploitation of children, commissioned a survey of sexual exploitation victims to find out the role of technology in trafficking. 63% of the survey participants reported being sold online⁴.

The Internet – A Platform for Recruiting

The internet is also being used by traffickers as a tool to aid in the recruitment of victims. Traffickers are utilising social media to gather information on victims and create false profiles to create virtual relationships in order to groom future victims for prostitution.

² M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015; p. 1.

³ <http://fightthenewdrug.org/by-the-numbers-see-how-many-people-are-watching-porn-today/> accessed today 01.12.2016.

⁴ https://www.wearethorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf p 19. Accessed today 30.11.2016.

Unfortunately, traffickers are brilliant social engineers. Kevin Mitnick, in his book, “The Art of Deception” details how social engineers gain the trust of their victims⁵. They gain access to private information using innocent sounding questions as a way to help the victim feel like they understand them, providing a false sense of intimacy. They intentionally find out what the victim’s dreams and desires are then offer the victim help to achieve this. Eventually they work to gain provocative photos of victims that can be sold and used to blackmail them, or to actually meet the victim. It is at this intersection of human manipulation and social technology that many fall victim to traffickers.

The Dark Web – The New Frontier of Human Trafficking

What has been described so far is human trafficking activity on the *surface web*. This is the part of the internet that can be readily accessed by search engines like Google and Bing. It is the place where most of our everyday internet activity occurs. However, there is more to the web than meets the eye. There is part of the internet that is more than 500 times the size of the surface web⁶. This is known as the *deep web* and it contains the non-searchable part of the web. Beneath this lies another subsection of the web called the *dark web*. It is the part of the internet that is kept intentionally hidden and provides the perfect cover for human trafficking activity.

The dark web near guarantees anonymity to its users through the use of multi-layered encryption technology called *onion encryption*. As the name suggests, access to onion encrypted websites (with the domain .onion) are passed through layers like an onion. At each layer the user’s IP address, the identifying address of a computer, is encrypted and passed to another volunteer server and hence the next layer. As the destination website only receives the last IP address in the route process, the website never actually knows who they are communicating with.

The dark web may be accessed by a readily available search engine called Tor⁷. Tor navigates these onion layers and leads the searcher to the desired website without any trace of who they actually are. Tor does not keep record of searches⁸ so there is no trace of activity at this stage either.

Other elements of the dark web include Hidden Wiki that provides a directory of what can be found of the dark web including the procurement of assassination services, arms dealing, human experimentation⁹ and paedophilia. A study by Gareth Owen at the University of Portsmouth found that 4 out of 5 searches on the dark web involve paedophile activity¹⁰. The dark web also has its own currency called Bitcoin that provides anonymous payment for services along with prepaid debit cards. Even tech giants like Facebook are beginning to make their services available through Tor¹¹.

⁵ K. D. Mitnick, W. L. Simon *The Art of Deception: Controlling the Human Element of Security*, “Wiley Pub” Publishing House, Indiana, 2002.

⁶ M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015; p. 2.

⁷ Warning: The dark web is accessed at your own risk.

⁸ E. Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015, p. 11.

⁹ M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015; p. 5.

¹⁰ <https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> accessed today 30.11.2016.

¹¹ <http://www.bbc.com/news/technology-29879851> accessed Today 01.12.2016.

HUMAN TRAFFICKING AS CYBERCRIME

Other Dark Web Activity

Whilst the dark web is being utilised for criminal activity it does also have a good side as does the surface web. It is essentially the human element that makes it for good or for evil. Tor was initially created by the US Naval Research Laboratory¹² in 2002 to communicate online anonymously. It proves useful to journalists, whistle blowers and government officials risking their lives to communicate information safely.

The dark web also attracts another group of people called *hacktivists* that protest outside of the boundaries of law. A hacktivist group called ‘Anonymous’ rallied together to hack into and lobby Lolita City, a website selling images of child abuse to paedophiles¹³. This group contacted the hosting company to remove the material and when they refused they publically exposed the details of more than 1,500 paedophiles.

Whilst on the surface this may appear to be a good thing, it was not done using legal methods and was more of a naming and shaming tactic and may have interrupted criminal investigations. However, it does show that the dark web does not provide guaranteed anonymity.

Cybercrime Counter Human Trafficking Efforts

There are some good advances in tools to fight cybercrime on the surface web and the dark web that should be noted.

Spotlight is a tool created by Thorn in partnership with Digital Reasoning. Spotlight scraps publicly available information from the internet, analyses it and uses it to help prioritise cases for law enforcement¹⁴. It focuses on child trafficking data and essentially increases the response time of police by providing concentrated data to work with. Lieutenant Chad Gremillion of the Louisiana State Police reported:

“Seeing Spotlight in action reinforces the idea that we can use technology for good. This is such an incredibly powerful tool in our effort to locate trafficking victims and get them connected to services. It’s also made our jobs easier in finding offenders, which is exactly what we did after identifying Karina. With the help of Spotlight, we not only arrested her trafficker, but he’s now looking at 30 years to life in prison. We couldn’t have asked for a better outcome for her and for this case.¹⁵”

With cybercrime being fairly recent, new groups are being established to monitor and provide accountability at a global effort. This is especially important as no one group owns the internet. In January 2014 the Global Commission on Internet Governance was established to articulate and advance strategic vision for the future of Internet governance¹⁶. Its key focuses include ensuring human rights online, freedom of expression and cybercrime cooperation.

¹² M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015; p. 3.

¹³ <http://www.telegraph.co.uk/technology/internet/8851242/The-Hidden-Wiki-an-internet-underworld-of-child-abuse.html> accessed today 30.11.2016.

¹⁴ <http://www.digitalreasoning.com/buzz/using-tech-to-find-victims-of-child-sex-trafficking.1719834> accessed today 30.11.2016.

¹⁵ <http://www.digitalreasoning.com/buzz/using-tech-to-find-victims-of-child-sex-trafficking.1719834> accessed today 30.11.2016.

¹⁶ E. Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015, p. vi.

The United Nation's International Police Organisation (INTERPOL) have created the International Child Sexual exploitation image database¹⁷ that is used by police globally. Google have been working with the National Center for Missing and Exploited Children (NCMEC) to adapt their copyright recognition program to detect child pornography¹⁸. Likewise, Microsoft have also worked NCMEC to create PhotoDNA to analyse large number of images quickly to detect modified versions of child pornography.

Recommendations

Clearly, fighting human trafficking in the virtual world is a new frontier that is constantly evolving. Human trafficking cannot be fought solely on a legal or technical basis. Prevention efforts need to focus on the intersection of inter-government co-operation, social engineering and technology. It involves human beings and therefore the corruption of human relationship is involved at one stage or another; whether it be the trafficker's promise of a better life or the abuse of physical relations through a John buying the services of his victim or a border official being paid to let someone through.¹⁹ The following recommendations should be considered as methods to further engage successfully in this area.

- Surveys similar to that commissioned by Thorn on the use of technology to recruit, groom and sell domestic minor sex trafficking victims²⁰ should become part of each nation's anti-trafficking strategy in order to understand how traffickers are using the internet to recruit and sell victims. This will provide qualitative data on keywords that traffickers are using that can then be used to fine tune the scraping and filtering of large amounts of publicly available information.
- Currently Spotlight is providing tools for law enforcement agencies in the US. This technology should be created on a national level in each country.
- Government funds should be directed towards anti trafficking efforts in each nation.
- National Helpline advertisements should be placed on search engine results for pornography. As traffickers utilise victims to place ads online, this method will alert victims to how they can access help²¹. Ads should be worded as they relate to the victim. That is, they should say "are you being forced to have sex with people so someone else gets money?" as opposed to "are you being trafficked?" Unfortunately, those that are being trafficked often don't realise that is what has happened so the terminology does not resonate with them.
- Global government collaboration is required for international, national and domestic law and accountability of internet usage. Anti-trafficking groups need to be included in the discussion for internet governance as they can contribute to the profiling of traffickers with their wealth of information and can help to identify trends in keywords. Internet governance needs to be guided by an understanding of the human side of security.

¹⁷ B. Westlake, M. Bouchard, R. Frank, *Comparing Methods for Detecting Child Exploitation Content Online*, "European Intelligence and Security Informatics Conference (2012)" Publishing House, 2012: p. 156.

¹⁸ B. Westlake, M. Bouchard, R. Frank, *Comparing Methods for Detecting Child Exploitation Content Online*, "European Intelligence and Security Informatics Conference (2012)" Publishing House, 2012: p. 156.

¹⁹ Luz Estella Nagle, *Selling Souls: The Effect of Globalization on Human Trafficking and Forced Servitude*, "Wisconsin International Law Journal, Vol. 26, No. 1, 2008" Publishing House, 2008, p. 133.

²⁰ https://www.wearethorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf accessed today 30.11.2016.

²¹ https://www.wearethorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf p. 31 accessed today 30.11.2016.

HUMAN TRAFFICKING AS CYBERCRIME

- Police organisations need to be trained at a local level on cybercrime activity and how to respond.
- NGOs need to be trained at a local level on cybercrime activity and how to respond. They can help to provide further qualitative cybercrime understanding well after cases are finished legal proceedings.
- Mutual Legal Assistance Treaties on cybercrime need to be formed between nations²².
- Government needs to work with private companies providing technology to gain access to information that will enable investigative policing to continue²³

Conclusion

Human trafficking utilises much of the technology available today. Human traffickers are actively utilising both the surface web and dark web to operate their crimes in both the sale and recruiting of victims. Whilst efforts to fight human trafficking as cybercrime are beginning there is much work left to do. This work requires the further understanding of the situation, development of technology, training of those involved as well as governmental cooperation on a global level. It is possible to break into these systems supporting the human trafficking underworld and both prevent cybercrime and hold its perpetrators accountable.

Bibliography

General

1. M. Chertoff, T. Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015;
2. E. Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015;
3. B. Westlake, M. Bouchard, R. Frank, *Comparing Methods for Detecting Child Exploitation Content Online*, “European Intelligence and Security Informatics Conference (2012)” Publishing House, 2012: pp. 156-163;
4. S. Kara, *Supply and demand: Human trafficking in the global economy*. “Harvard International Review” Publishing House, Summer 2011, p 66-71;
5. Luz Estella Nagle, *Selling Souls: The Effect of Globalization on Human Trafficking and Forced Servitude*, “Wisconsin International Law Journal, Vol. 26, No. 1, 2008” Publishing House, 2008 pp. 131-162;
6. P. Åström . *Beyond all Tolerance: A growing problem demanding new counter-measures*, “Save the Children” Publishing House, Sweden, 2004;
7. K. D. Mitnick, W. L. Simon *The Art of Deception: Controlling the Human Element of Security*, “Wiley Pub” Publishing House, Indiana, 2002;

Speciality works and related Legislation

1. United Nations, *Protocol to Prevent, Suppress and Punish Trafficking in Persons*, 2000; Article 3, paragraph (a)

Electronic Sources

1. <http://assets.globalslaveryindex.org/downloads/Global+Slavery+Index+2016.pdf>

²² E. Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015, p. 10.

²³ E. Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, “Center for International Governance Innovation and Chatham House” Publishing House, Canada, 2015, p. 11.

2. <http://fightthenewdrug.org/by-the-numbers-see-how-many-people-are-watching-porn-today/>
3. https://www.wearethorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf
4. <https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/>
5. <http://terrorismanalysts.com/pt/index.php/pot/article/view/513>
6. <http://www.digitalreasoning.com/buzz/using-tech-to-find-victims-of-child-sex-trafficking.1719834>
7. <http://www.telegraph.co.uk/technology/internet/8851242/The-Hidden-Wiki-an-internet-underworld-of-child-abuse.html>
8. <http://www.critic.co.nz/features/article/3629/how-to-navigate-the-deep-web>
9. <http://www.nydailynews.com/new-york/nyc-crime/founder-rentboy-pleads-guilty-prostitution-charge-article-1.2821488?platform=hootsuite>
10. <http://www.latimes.com/local/lanow/la-me-ln-backpage-ceo-arrested-charged-20161006-snap-story.html>
11. <http://www.bbc.com/news/technology-29879851>