CASIS - VANCOUVER - ACERS

SAPERE AUDE

THE ROLE OF THE DARK WEB IN THE CRIME AND TERRORISM NEXUS

Date: November 15, 2018

Disclaimer: This briefing note contains the encapsulation of views presented throughout the evening and does not exclusively represent the views of the speaker or the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

On November 15, 2018, the Canadian Association for Security and Intelligence Studies (CASIS) Vancouver hosted its tenth roundtable meeting which covered "The Role of the dark web in the Crime and Terrorism Nexus." The presentation was hosted by Dr. Richard Frank, an assistant professor in the School of Criminology at Simon Fraser University, as well as the Director of the International CyberCrime Research Centre (ICCRC). In the presentation, Dr. Frank began by explaining the operations of the dark web, and then moved on to discuss why the dark web cannot just be shut down, as well as actions law enforcement (policing) could take in order to counter the activities on the dark web. The subsequent roundtable discussion opened with an analysis of the operations of *Silk Road*, an online marketplace on the dark web that specializes in the sale of illegal drugs, weapons, and stolen identities. The topics of interest in the discussion were the effects of internet-based trade of illicit goods on organized crime and local drug markets, in addition to whether the dark web can be used constructively.

NATURE OF DISCUSSION

Presentation

The presentation first focused on describing the operations of the dark web. Dr. Frank emphasized the tight encryption throughout the dark web in order to demonstrate the difficulties in shutting down its operations. Throughout the presentation, Dr. Frank highlighted that combatting the dark web requires going around its security, rather than trying to attack the core of its operations. It is argued that the dark web is becoming increasingly difficult to attack as many of the loopholes previously exploited in order to combat the illegal market have now been fixed.

Roundtable

The roundtable had a key focus in discussing the impacts on organized crime and drug markets at the local level from trades within the dark web. The role of technology, technical barriers, and the characteristics of the individuals using the dark web were collectively discussed in order to determine how the dark web influences criminal activities.

BACKGROUND

Presentation

Dr. Frank explained that encryption is the core of the dark web, allowing users to communicate in anonymity. The internet is viewed as three layers: the surface web, deep web, and dark web. The surface web is the open web that is available to anyone while the deep web is more restricted and not accessible through mainstream search engines. The dark web is only accessible through certain vehicles and may present malicious content.

Dr. Frank explained that the dark web, although difficult to access, still runs on public internet infrastructure using specialized networks such as, *Tor, Freenet, GNUnet, I2P, Retroshare,* and *Oneswarm*. Access to websites via such networks is not difficult, provided a user knows how to find their desired website. The Tor network, one of the most popular networks for accessing the dark web was discussed in detail by Dr. Frank. The operations of the Tor network to maintain anonymity rely on the creation of random paths in order to bounce traffic through various nodes. The content of a message remains encrypted throughout the node-to-node bounce until it reaches the recipient.

According to Dr. Frank, the dark web has three main uses: communication, visiting internet sites, and using hidden services. To elaborate, the dark web allows users to communicate through chat programs that maintain anonymity of their identity, as well as confidentiality of their messages. The second use of the dark web allows users to remain anonymous and visit internet sites that may be prohibited in their country. Thirdly, the dark web allows for the use of hidden services that exist only within the given network; in other words, both the user accessing the site and the website itself remain anonymous.

Subsequently, Dr. Frank discussed the issues present in the dark web, as well as solutions that have been devised. The two main problems present in the dark web are arguably trustworthiness, and identity. The former is an issue because as the identity of the seller remains anonymous, there is no guarantee that the seller will honour the deal made with the buyer. The latter is an issue because at some point, the buyer will have to identify oneself to some degree, in order to receive their purchased product. The issue of trustworthiness was solved with the creation of Silk Road, a website that required mandatory feedback by the buyer. By requiring feedback on the seller's business, the website is able to establish trust in an anonymous buyer-seller relationship.

Given the degree of security present in the dark web, Dr. Frank argues that it's nearly impossible to break through the heavy encryption. Instead, as he proposed, a more viable approach is to go around the mechanisms of encryption. In light of this, potential approaches to combat Dark Web activity are i) to attack the vulnerability of the encryption or ii) to attack the encryption process itself. The validation of this methodology can be illustrated in the successes of shutting down the Silk Road, Silk Road 2.0, Hansa, and AlphaBay. Another example of going around the security is *Operation Bayonet*, where the Dutch police took over the market of the dark web. This not only took down many of the users on the dark web, but more importantly, it arguably succeeded in undermining the trust in the market itself.

In the last portion of the presentation, Dr. Frank introduced the notion of artificial intelligence (AI) in order to assist with combatting the dark web. Research is being done in order to use machine learning to predict the content of webpages on the dark web. In terms of methodology, the artificially intelligent system will be given a large number of webpages on the dark web which it will then categorize and use in order to build a model website. Subsequently, it will apply its model website in order to predict the maliciousness of new websites. If the system determines that the website is concerning, it will tag the website and forward it for an in-depth, human analysis. The combination of artificial and human intelligence is hoped to be more efficient in taking down malicious websites, as artificial intelligence will filter the websites required for human analysis.

Roundtable

The roundtable opened with a discussion of the influence of internet-based trade of illicit goods on the local market. In response, the issue of technological barriers was raised. It was brought to light that currently, those who partake in internet-based trade are usually those who are technologically savvy because the knowledge required to access and carry out a transaction on the dark web is quite different compared to the surface web, primarily due to access of the dark web and the form of payment used (bitcoin). Due to the lack of widespread technical knowledge, the dark web currently may not have a strong influence on local drug markets and organized crime. However, if the dark web is made more user-friendly in the future, its influence on local trade and organized crime could potentially change.

Secondly, the difference between online and local drug markets was discussed. Where the price of a drug sold in the local drug market fluctuates depending on factors such as geography and demand, the price of a drug sold on the dark web is not subject to such factors and therefore static regardless of the buyer's region. Despite the anonymity provided by the dark web, it can be argued that some sellers do not ship to certain countries in fear of border regulations while some buyers prefer to purchase within their own country for the same reason.

Thirdly, the efficiency of artificial intelligence and machine learning systems on the generation of intelligence assessments was brought up. It was discussed that such systems will still be limited in their use as they will not be able to interact with the websites as analysts themselves can. It was argued that although an AI can be effectively employed to perform tasks such as mining large quantities of data, the final assessment will still require a measure of human oversight. Consequently, artificial intelligence will only supplement, and not replace human analysis.

Lastly, discussion on the constructive purposes of the dark web suggested that the dark web may be useful for non-malicious purposes. It was brought to attention that the dark web was used during the Arab Spring, which allowed users to promote their views anonymously and without state oversight. In addition, the dark web can be useful for membership purposes, as well as maintaining anonymity of chats and emails that may contain sensitive content.

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Presentation

- The internet is viewed as three layers: the surface web, deep web, and Dark Web. The surface web is the open web that is available to anyone while the deep web is more restricted and not accessible through mainstream search engines. The dark web is only accessible through certain vehicles and may present malicious content.

- The dark web runs on the public internet infrastructure using specialized networks such as, Tor, Freenet, GNUnet, I2P, Retroshare, and Oneswarm. The Tor network is one of the most popular networks and it maintains user anonymity rely by creating random paths in order to bounce traffic through various nodes. The content of a message remains encrypted throughout the node-to-node bounce until it reaches the recipient.
- The dark web can be useful for communication, visiting internet sites, and using hidden services.
- Given the degree of security present in the dark web, Dr. Frank emphasized that it’s nearly impossible to break through heavy encryption; therefore, a more viable approach is to go around the mechanisms of encryption.
- Artificial and human intelligence may be useful in combating the dark web. For example, the AI can extract a large number of webpages on the dark web which it will then categorize and use in order to build a model website. It will then apply the model site to predict other malicious websites, tagging them and forwarding them to human analysts for review.

Roundtable

- The technological barriers involved with access to the dark web and the processing of transactions may contribute to preventing the dark web from influencing local drug markets and organized trades. However, if the dark web is made more user-friendly in the future, its influence on local trade and organized crime could potentially change.
- The prices of products sold on the dark web are not subject to factors that may influence the prices of the local market, such as geography and demand. The transactions on the dark web may currently be limited due to border regulations that may hinder sellers to ship to certain countries and possibly motivate buyers to purchase within their own country.
- AI systems can be employed to perform tasks such as mining large quantities of data, but the final assessment will still require human oversight. Consequently, artificial intelligence will only supplement, and not replace human analysis.
- The dark web does not necessarily need to be used for malicious purposes. Examples for this are its use in the Arab Spring, as well as its usefulness in maintaining anonymity of chats and emails that may contain sensitive content.

WEST COAST PERSPECTIVES

Presentation

- If activity on the dark web is heightened, how such activity will influence the dynamics of the country is a question that remains unanswered. One possibility is that the illegal weapons and drug market may influence society negatively. Another is that the easy availability of illegal weapons and drugs may no longer make these goods as appealing to individuals.
- As it is becoming more difficult for law enforcement to find loopholes and shut down the activity of the dark web, novel methods of combating such a platform are suggested. As AI has been proposed to be a viable option in fighting against the dark web, it could be possible that job prospects in the field of cybersecurity may increase in the future.

Roundtable

- If an increased number of buyers and sellers begin to use the dark web, there may be the potential for increased illegal activity concerning the sales of particular goods. The relationship between the increased availability of drugs and weapons is one to consider as over half of criminal groups currently derive their revenue from illegal drug sales.
- Provided that the drugs ordered from the dark web are able to bypass security, the issue of concern is how such an increased availability of illegal drugs will influence usage in the country. If drugs are possibly more readily available for individuals to exploit, one possibility is that drug abuse may increase. The country has seen the outcomes of the fentanyl and opioid crisis - if it became easier to obtain illicit drugs, will the country's economy suffer? Substance abuse costs healthcare services nearly $8 million and with an increase in the availability of illicit drugs, the number may go up even more.
- Provided that the weapons ordered from the dark web are able to bypass security, the issue of concern is how such an increased availability of weapons will influence violent activities in the country. With relation to gang violence, if access to weapons becomes easier, then gang violence may become more prominent than it currently is. With respect to the general public, the purchase and use of unregistered guns on the streets may result in more violent and frequent shootings, in addition to arguably increased fear in the general public, as seen in countries with relaxed gun laws.

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University

Available from: https://jicw.org/