# Exploring the Interactional Theory: A Theoretical Exploration of the Dark Web's Impact on Delinquent Behaviour

of

Michael Magnante

A thesis submitted to the
School of Graduate and Postdoctoral Studies in partial
fulfillment of the requirements for the degree of

**Masters of Arts in Criminology**

**Faculty of Social Science and Humanities**

University of Ontario Institute of Technology (Ontario Tech University)

Oshawa, Ontario, Canada

August 2021

**THESIS EXAMINATION INFORMATION**

Submitted by: Michael Magnante

**Master of Arts** in **Criminology**

Thesis title: Exploring the Interactional Theory: A Theoretical Exploration of the Dark Web's Impact on Delinquent Behaviour

An oral defence of this thesis took place on August, 4, 2021 in front of the following examining committee:

**Examining Committee:**

| | |
|---|---|
| Chair of Examining Committee | Dr. Carla Cesaroni |
| Research Supervisor | Dr. Steven Downing |
| Examining Committee Member | Dr. Jordan Harel |
| Thesis Examiner | Dr. Amir Mostaghim |

The above committee determined that the thesis is acceptable in form and content and that a satisfactory knowledge of the field covered by the thesis was demonstrated by the candidate during an oral examination. A signed copy of the Certificate of Approval is available from the School of Graduate and Postdoctoral Studies.

**Abstract**

Throughout the years, modern issues of delinquent behaviour have evolved and shifted from the advancements of technology and the development of the virtual world. Despite the possibility for this connection, research has exclusively concentrated on the disruption of product flow. This study looks to explore the development and significance of delinquent behaviour within the dark web. Using Thornberry's (1987) Interactional theory, the study explores how the dark web manifested as a marketplace, illegal tool-kit, and virtual community impacts delinquent behaviour. The study conducts an exploratory case study on the illicit Whitehouse market to explore while the interactional theory is a useful theoretical approach that can account for the dark web as a marketplace, illegal tool-kit, and virtual community impacting delinquent behaviour, it fails to account whether or not the dark web impacts the weakening of normative social bonds to conventional society.

**Keywords:** darknet; deviance; marketplace; illegal tool-kit; community

## AUTHOR'S DECLARATION

I hereby declare that this thesis consists of original work of which I have authored. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize the University of Ontario Institute of Technology (Ontario Tech University) to lend this thesis to other institutions or individuals for the purpose of scholarly research. I further authorize University of Ontario Institute of Technology (Ontario Tech University) to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research. I understand that my thesis will be made electronically available to the public.

Michael Magnante

## STATEMENT OF CONTRIBUTIONS

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication. I have used standard referencing practices to acknowledge ideas, research techniques, or other materials that belong to others. Furthermore, I hereby certify that I am the sole source of the creative works and/or inventive knowledge described in this thesis.

**ACKNOWLEDGEMENTS**

I would first like to thank my supervisor, Dr. Steven Downing, for his immense support and guidance throughout the last year. Your support, help, and guidance were able to help and strengthen my research and give me the motivation to continue pursuing and completing my work. You have been an incredible mentor, and I appreciate all that you have done for me.

I would like to thank my supervisory committee, Dr. Jordan Harel, for all the insight, encouragement, and direction for strengthening my research topic. You have greatly contributed to the research process and have been an incredible mentor that has made me a better researcher. The research could not have been completed without your expertise and support.

I would like to thank my great friend Ejaz Thawer who assisted me in the editing process and provided great assistance and expertise. I could not have been able to complete my work without his help. I am truly blessed to have a friend like him that provided me with the unlimited support that he did.

I would like to thank my amazing family and girlfriend Candice, who helped me with the challenges, provided me with the constant encouragement and motivation to push in order to complete my work. Thank you all for the unlimited affection and support. I am blessed to have a family like you.

**TABLE OF CONTENTS**

## LIST OF TABLES

### CHAPTER 5

## LIST OF FIGURES

### CHAPTER 5

## LIST OF ABBREVIATIONS AND SYMBOLS

| | |
|---|---|
| WHM | Whitehouse Market |
| US | United States |
| VPN | Virtual Private Network |
| PGP | Pretty Good Privacy |
| DDoS | Distributed Denial of Service Attack |

# Chapter 1: Introduction

Modern criminological research has focused primarily on analyzing the causes and evolution of influences on individual behaviour. Existing research in this domain has primarily been oriented towards understanding the underlying sources, drivers, and predictors of deviance. As Childs, Sullivan, and Gulledge (2010) state, it is clear that research documenting the causes of deviance must explain not only the ebb and flow of criminal careers but also the evolution of social influences on delinquent behaviour. Embedded in numerous theoretical frameworks advanced within the field of developmental criminology, these critical factors help to understand what guides individual choices and the impact of their environments and group associations. As Catalano and Hawkins (1996) explain behavioural development and social influences impact causal processes that underpin deviant behaviours.

The underlying dynamics of delinquent behaviour have transformed substantially throughout the years. One of the primary shifts has been precipitated by advancements in technology and the subsequent development of the virtual world. Encapsulated in the weaponization of cyberspace, the Internet has essentially served as the foundation for the emergence of new outlets of deviance. In this sense, virtual spaces are used by various delinquent users, such as drug or arms dealers, to network and form clandestine underground markets for a vast array of illegal activities (Krebs, 2017). Stalans and Finn (2016) explain that the online world is differentiated by its provision of a low-risk, high reward environment that has made it much easier for individuals to engage in criminal activity. This significant increase in engagement in cybercrime is principally attributable to the increase of engagements in the culture of crime, socialization, and freedom from self-control and external forces (Stalans & Finn, 2016).

The differences (or lack thereof) between cybercrime and traditional crime pose a conundrum about whether or not new theories or approaches are even necessary for the study of cybercrime. It may not be that cybercrime differs from traditional causes of crime, but rather that anonymity and technological advancements have altered human interactions and increased opportunities for criminal exploitation (Grabosky, 2001). Perhaps similarfundamental impacts and causes of criminality still exist, but cybercrime introduces new dimensions that drive motivations, opportunities, and deviance. It is important for a new theoretical contribution to explain these dynamics of cybercrime, as Grabosky (2001) explains, anonymity and exchanges of digital currencies can allow individuals to mask their true identities online, and raise the possibility of transnational crimes. Overall, the answer should not be to focus on whether or not there is a need for new approaches to study the impact of cybercrime, but focus on how conventional street crime has advanced through the use of the virtual realm. Furthermore, the question might not be how it differs but rather how the variety and number of opportunities have expanded in an exponentially changing and expanding world, as indeed, computing and communication advances create parallel opportunities and risks for prospective offenders (Grabosky, 2001). Therefore, it may not be about identifying how cybercrime is different from traditional causes of crime, but rather how cybercrime has evolved, altered, and impacted the motivations and influences of previous traditional causes of crime.

The most significant contributor to the contemporary escalation in cybercrime is the emergence of the dark web, an underground network below the confines of the surface web used to obtain operational freedom and express criminogenic desires. As the most extensive anonymous environment ever created, the dark web masks activities through complex encryption and routing channels that enable users to freely search the web without being tracked or monitored (The Tor Project, 2018). Despite the fact that alternative browsing systems (including I2P and Freenet) allow users to gain access, in most cases, Tor is the central browsing tool used, as a majority of dark web sites are found to apply the Tor encryption code. Tor accesses the underground network

anonymously by publishing and searching content through onion/hidden services (Jardine, 2018). The information is received in much the same way as the surface web but breaks up the direct connection through encrypted channeling tunnels to allow users to remain anonymous. As a result, Tor is understood to be a mechanism that covertly reads onion/hidden services or access explicit websites without leaving traces (Jardine, 2018).

Widely considered to constitute a virtual safe haven where users engage in illicit activities, the dark web is often framed by researchers as a platform that heightens and drives criminality. As an indicator of this rise in criminal activity, the growth of darknet markets has been enabled by various technological characteristics, such as encryption, anonymity, and cryptocurrency, to engage in illicit activities and behaviours (Holt, 2017). Notably, the tunnelling technology that underpins the anonymous quality of the darknet is seen by Holt (2017) to amplify the threat of increased illicit marketplaces and criminological activity. Moore and Thomas (2015) conducted a study where they located (in a mere five-week period) over 2000 dark web sites geared towards facilitating illicit activity. Reinforcing these authors' findings, McGuries (2019) also documented an increase of more than 20% in illicit activity occurring on the dark web in 2016. In essence, the rising popularity of the underground network has undergirded its transformation into an effective hub for illicit activity and operations. As, Shilito (2019) states, the dark web is fundamentally changing how crime is conducted.

The underground network has fostered clandestine illegal communities, which provide services ranging from the sale of unlicensed firearms and drugs to perpetuating human trafficking and targeted assassinations. Notably, the more widespread usage of the dark web has been found for the movement of drugs, financial attacks, and fraud (Stalans & Finn, 2016). The dark web has thus equipped users with the tools to create virtual markets for confidential buyers and sellers. As Stanlan and Finn (2016) describe, the dark web has created new ways to facilitate deviance and illicit activity through technological advancements that have increased encryption to mask identity. It has also created Dark

forums, chat rooms, and virtual markets have gained significant traffic due to the ease with which users can connect and communicate while keeping conversations or transactions private and untraceable (Krebs, 2015). Elements of online anonymity, layers of encryption, association with peers, and protection of information have collectively increased individuals' opportunity to engage in delinquent behaviour, and fortified bonds to deviance. While opportunities have increased, the extent research has yet to assess how the dark web may manifest bonding mechanisms between delinquent actors and darkweb markets and communities associated with them. The theoretical approaches of studying the dark web has mostly focused on either how it creates power and freedom for its users and creates a public perception that develops less constraints and affordances to what an individual can do on the virtual net. While, it also has been focused on how the dark web has created controversial hyper-private environments that have enhanced complex systems that provide extreme privacy for both marketers and consumers. As, Thomas, Salge, Karahanna, and Hulland (2019), state much research has focused on the shift of this nature of the dark web and how its privacy-focus has altered a variety of information sharing and protection practices that have been increasingly adapted by consumers.

Despite the outlined theoretical framework linking the dark web to deviance, a strikingly inadequate amount of research has been dedicated to comprehensively exploring this connection. As Holt (2017) has pointed out, most studies have focused on the descriptive portion of cyber-specific markets, where the research has exclusively concentrated on the disruption of product flow. Comparatively, little research has been geared towards exploring the dark web's direct influence on users' propensity to engage in delinquent behaviour, and the reciprocal effects that impact increased delinquent behaviour over time. Holt and Bossler (2014) illustrate that there has been a significant shift in how humans utilize computer technology, specifically as it pertains to their facilitation of criminal activity over the last few decades. Consequently, a substantial amount of research remains to be conducted in order for policymakers and law

enforcement agencies to truly understand both the increasing popularity of the dark web and the network's overarching influence on deviance.

The Current Inquiry

The current inquiry of the research study has three primary objectives:

1. Exploring the interactional theory's tenets on social learning and social control and determining whether they can account for the concepts of marketplace, illegal tool-kit, and community impacting delinquent behaviours.
2. Conducting an explanatory case study on the Whitehouse market and using the data collected to analyze the three prongs of marketplace, illicit tool-kit, and community and their impact on deviance.
3. Laying the foundation for a new theoretical framework to understand the dark web, that accounts for a new analysis on focusing on emerging delinquent factors and behaviours within the online environment

The purpose of this study is to explore the development and significance of deviance within the dark web. The study looks to explore more of a theoretical explanation of these underground networks, foster reciprocal cycles on delinquent behaviour, and create dynamics that can directly lead to individual change in behaviour (strengthening or weakening) and normative orientation (Thornberry, 1987). Thornberry's (1987) interactional theory will be used as the theoretical model with which to further illuminate understandings of the dark web as a marketplace, illegal tool-kit, and online community, while concomitantly discerning how the network impacts its users' social bonds, values, and prospects of engaging in delinquent behaviour. Bossler and Holt (2014) explain that the expansion of research into online marketplaces and cyber-related crimes could enhance our knowledge and understanding of the social impact of these virtual networks. Therefore, exploring how these markets are used and how these communities are formed can aid in the overall understanding of these underground networks on illicit activities and emerging delinquent behaviours.

This analysis will utilize Thornberry's (1987) interactional theory to investigate the reciprocal effect on the relationship of social control and social learning processes on delinquent behaviour. Thornberry (1987) combined elements of Hirschi's (1969) social control theory and Akers (1985) social learning theory to study delinquent behaviour emerging and conventional bonds weakening in an amplifying loop. Thornberry's (1987) theory has predominantly been used to account for deviance resulting from the freedom afforded by the weakening of one's bonds to conventional society and presented in an interactional setting where delinquent behaviour can be learned and reinforced. Composed of a set of explanatory models that explicitly describe deviance as both an outcome and predictor of illicit activity, the interactional theory constitutes an ideal framework for developing and examining new associations (Hoffman, Erickson, & Spence, 2013). Thornberry (1987) suggested that delinquent behaviour occurs as a byproduct of social interaction and is consequently best explained by models that focus on interactive social processes.

The research study will be using the tenets of social learning and social control from Thornberry's (1987) interactional theory to explore how the dark web as a marketplace, illegal tool-kit, and community impacting delinquent behaviour. Employing Thornberry's interactional theory, the study explores precisely how, through processes of social interactions, the specific elements of the dark web play a critical role in potentially increasing the networks' influence on delinquent behaviour and the internalization of pro-delinquent norms (Thornberry, 1987). The dark web increases its users' association with peers who participate in underground markets for similar reasons (particularly buying and selling illicit products). That is, delinquent behaviour emerges within these underground markets and is understood to represent a corollary of social factors of peer association and interactions with delinquent peers. Operating from this foundational premise, the tenets of social control and social learning theory theoretically dissect and emphasize Thornberry's (1987) interactional model to illustrate the reciprocal relations between the

dark web marketplace, tool-kit, and community, and their collective influence on the network's users' involvement in delinquent peer associations and adoption of delinquent values.

The major contribution of this research study will be on the theoretical analysis on the dark web and how it can cause/impact delinquent behaviour while possibly decreasing conventional social bonds in an amplifying loop. The research will be conducting an explanatory case study of the illicit Whitehouse marketplace. Despite being considered a more miniature marketplace on the dark web, the Whitehouse market contains an active forum where a substantial amount of user engagement occurs. Conducting an exploratory case study will allow the paper to strive to determine whether Thornberry's interactional theory is applicable to analyze delinquent behaviour stimulated by one's engagement within the dark web. Most importantly, if the interactional theory can empirically explore the dark web as a marketplace, illegal tool-kit, and community being impactful influences on emerging individual delinquent behaviours, bonds, and values.

The research study will focus on exploring the marketplace, illegal tool-kit, and community impacting delinquent behaviour in the dark web. The marketplace sector will be investigated to discern how elements of Internet-mediated communication, provision of anonymity, encryption and the development of echo chambers impact reciprocal relations on opportunity and choice to commit delinquent activities and behaviours. The ensuing discussion further clarifies how these elements of Internet-mediated communication, provision of anonymity, and echo chambers within the marketplace combine to form an amplifying loop of emerging pro-delinquent behaviour and values. Multiple mechanisms will also be explored as to why tool-kits in the dark web can impact delinquent behaviours. Primarily, the focus will be on how users may use these tool-kits to learn new or advanced pre-existing delinquent behaviours from technology or peer group association. This idea is examined in two distinct ways. One centres understanding

exactly how individuals learn the technical aspects and how that delinquent peer associations reinforce members' delinquent behaviours and values. Lastly, beyond illustrating how these communities are built through the strengthening of delinquent values, the study discerns how such associations contribute to the formation of an amplifying loop, whereby individuals share information, practices, and recommendations concerning delinquent behaviour, and solidify their social bond to delinquent norms. While investigating how social structure characteristics and values can help conceptualize side-by-side differentiation of ideas, desirable goals, and market values. The analysis will still result in some degree of results of whether the entirety of the interactional theory can be used to explain how the dark web impacts reciprocal effects on delinquent behaviour and weaken normative bonds to conventional society.

The research will be starting with a review of the existing literature pertaining to the dark web based on current classification, major roles, current understanding, and current research focus. After reviewing the current literature, the paper will move on to discussing Thornberry's interactional theory and how this paper incorporates the theory and the significance of where it slots into the research. Then the paper will move to outlining the methodological approach and go ahead with the exploratory case study and content analysis of the Whitehouse market. Finally, the paper will discuss the implications of the findings, and address any limitations of the study, including while the interactional theory is a useful theoretical approach that can account for the dark web as a marketplace, illegal tool-kit, and community impacting delinquent behaviour, it fails to account whether or not the dark web impacts the weakening of normative social bonds to conventional society.

## Chapter 2: Literature Review

The Internet represents an interactive environment where individuals can quickly and easily communicate with one another. It has enabled the expansion of boundaries and individual capabilities in the digital world. The dark web is no different, as it is a subset network that expands an individual's capability of what they can do and say while decreasing their accountability for their actions. The main difference between the surface web and the dark web is that the latter enables its users to remain unidentifiable, and thus reduces the chances that they will be held accountable for their actions online. Notions of the dark web's expanding boundaries and prioritization of anonymity are key features of modern complicated, messy, and exciting conversations within cybercrime research (Kinklea, 2017).

### Classification of Dark Web Spaces

Alongside the surface and deep web, the dark web is classified as one of the three recognized spaces found within the Internet. The surface web is known as the more traditional network that is readily available to the general public and holds its users to the most accountability based on it being a visible network where privacy is intrusive and where user data can be easily collected (Bernstein, Marshall & Zvolensky, 2011). Alternatively, the deep web houses certain virtual regions that are not publicly accessible and are restricted by authentication requirements (Bernstein et al., 2011). The dark web is predominantly characterized as a hidden network found outside the traditional search engines, and that require special software to gain access. The main difference between the dark web and its counterparts is that the former network allows its users to become unidentifiable within the network and reduce user accountability of their actions and activities they conduct.

The encrypted features of the dark web allow for the decrease of potential opportunities for one's activities online being detected and limits the ability for external sources to detect/track one's online activities. Kinklea (2017) explains that the dark web

contains intentionally concealed content and can be used to disguise illegal and malicious activity. This central feature undergirds the dark web's status as an ideal platform upon which individuals conduct/facilitate illicit transactions. Consequently, the dark web has gained popularity as a direct result of the technological tools it employs to enable users to remain anonymous, increase opportunity for illicit operations, and have activities masked from being traced back to individual IP addressees. The surface and deep web do not enable their users to remain anonymous in the same way that the dark web does in order to protect ones privacy and security from outside external sources. Thus, the number of individuals using the dark web to facilitate illicit transactions has increased substantially in recent decades. Many who participate in illicit activity on the dark web rely on the network to not only carry out illegal operations, but drastically reduce their chances of being detected and tracked by law enforcement (Kinklea, 2017).

The dark web relies on network searching systems like the onion router (Tor) to allow users to remain hidden and anonymous in the underground network. The system allows the network to both mask one's identity and create end to end encryption to effectively render logs of the user's movement non-existent (Krebs, 2015). The system encrypted technology permits the emergence of forums, chat rooms, and communication services that collectively aid in the planning, marketing, and coordinating of illegal activities (Krebs, 2015). In this sense, these technological advancements of encryption and anonymity have created advancements in the utilization of criminal enterprises and operations to underpin the dark web's increasing popularity, as they serve as the basis for users' ability to anonymously sell and trade illicit goods.

The dark web has become an essential tool that overlays and distributes systems from under the global Internet. Hughes et al. (2006) explains that these networks provide functionality to allow users to empower themselves to undermine the tracking efforts of law enforcement agencies. According to Quinton (2014) notes that Tor secures the privacy of its users by allowing them to access/share sensitive and dangerous information

without being traced (or whilst remaining anonymous). Tor is thus the most used search engine to gain access to the dark web, and to its various chat rooms and underground forums that allow users to remain hidden but also allow to engage/conduct criminal activity (Quinton, 2014). Overall, the network enables individuals to engage and conduct illegal activities based on the encrypted technology that makes it virtually impossible to detect when users are entering the network and when they are leaving.

While Tor is not the only network through which individuals may gain access to the dark web, other search engines like I2P and Freenet similarly allow entry into this underground virtual space, but Tor remains the most popular browser used for this particular purpose, as most sites imply its distinct encryption technology (Kinklea, 2017). An analysis conducted at the University of Portsmouth found that there were approximately 45,000 hidden services online that were directing hidden sites through the Tor browser (Schneier, 2013). Schneier (2013) bolstered these findings by determining that Tor was found to traffic over 5,225 live websites, of which 1,547 contained illicit content. The dark web has remained prominent precisely due to its lack of central servers or control points through which to track users (Tanebaum & Van Steen, 2007). The inability to shut down is seen as extremely beneficial and effective tool for underground users because that major governments and law enforcement agencies are unable to mark where the activities are starting and ending, making it almost impossible to regulate user activities and operations within the network (Tanenbaum & Van Steen, 2007).

It has become increasingly difficult for law enforcement agencies to track and regulate because of the secure means of communication and untraceable infrastructure (Chertoff & Simon, 2015). Ciancaglini (2013) states that many activities performed on the dark web are unlikely to worry a huge deal from potential shut downs due to high secrecy levels of protection and security protocols to increase the difficulty of external forces spotting and observing. It becomes a lucrative environment for individuals to conduct illicit activity as it is relatively free from government control (Weimann, 2016).

It becomes convenient for criminals and organizations to conduct illicit activity over the dark web because sites can come online and then disappear on a regular basis, making it difficult to track virtual sites and users identities (Ciancalini, 2013).

Major Roles of the Dark Web

The dark web has played a significant role in encryption and becoming a focal point of illegal activity and the prominent virtual platform upon which individuals distribute illicit substances. Research has found that the network contains a variety of enabling infrastructure, including botnets, markets for trade, hackers for hire, private communication, coordination for attacks, DDOS attacks, and data breaches (Winkler & Gomes, 2016). In essence, the dark web has become a significant part of the novel, most evolved strain of cybercrime.

As the network enables users to conduct illicit transactions anonymously, the emergence of the dark web has fundamentally altered the way illegal goods and services are distributed online. The underground network has changed the way criminals facilitate crime, resulting in unmitigated issues for law enforcement (Shilito, 2019). According to Shilito (2019) the dark web has played a significant role in cybercrime and the distribution of illicit products in four ways. For one, it creates a countermeasure to confiscating crime proceeds, which create massive hurdles in law enforcement and policymakers measurements to counter act criminal activity (Shilito, 2019). Second, it has led to the expansion of boundaries to traditional crimes to incorporate regional and international networks, making it more difficult to investigate into criminal enterprises within the dark web (Shilito, 2019). Third, it has increased the jurisdiction of law enforcement and government authority agencies to struggle to counteract movement of illicit products circulating within the dark web and being easily sold to various outlets with little resistance. Finally, it has facilitated the evolution of traditional criminal enterprises, whose leaders weaponize modern technology to circumvent official detection efforts (Shilito, 2019).

The dark web has served as a platform upon which users distribute illicit products, launder currencies, either by buying or downloading security or hacking software, and distribute illegal sexual content (Spitters, Verbruggen & Staalduinen, 2014). The marketplaces that have emerged on this underground network have generated significant profits. As one of the first major markets to be created, Silk Road grew to accumulate upwards of 1.2 million dollars per month in sales (Christian & Soska, 2013). A majority of this revenue is connected to the sale of illegal substances and narcotics (Christian & Soska, 2013). The dark web also serves as a forum for conversation, coordination, and action, where many users relied on it to carry out their illicit operations (Kinklea, 2017). A wide variety of crimes, including the movement of drugs, sales of weapons, sales of exotic animals, and stolen goods for profit, occur within these underground markets (Kinklea, 2017).

The dark web has been known to be used to host chat rooms, communication services or distribution sites. The network effectively provides a platform for individuals to sell, distribute or advertise illicit products. Users conduct illegal activities without regard for traditional borders and boundaries of the offline world, as individuals have the opportunity to move products freely online and exploit the laws attempting to counteract illegal operations, as within these borderless markets users can freely conduct illicit activity without the heighten risks of being caught (Hayes, Cappa & Cardon, 2018). The dark web has become known to heighten the opportunities for illegal enterprises and increases users ability to operate online from the absent of fear from prying eyes. Additionally, it has encouraged anonymous consumers to use bitcoin as their preferred currency to further mask illicit transactions (Hayes et al., 2018). Academics and investigate agencies have had limited luck in their attempts to uncover the intricacies of transactions on the dark web, as the quality of vendor security and cloaking practices has improved over time (Hayes et al., 2018). Most notably, layers of encryption have provided both enhanced safety and privacy to vendors and customers alike.

One of the most popular and used cryptocurrencies to complete transitions has been found to be the use of bitcoin. Bitcoin is an encrypted currency that all dark web users utilize to complete transactions. Through his findings, Chertoff (2016) describes that bitcoin is viewed as the standard currency of various underground markets because of its signature algorithm and ability to be stored in hidden digital wallets. The use of cryptocurrency and crypto wallets are strategically designed to be difficult to track back to the individual who used and spent them (Chertoff, 2016). The development of bitcoin itself was geared towards both mirroring and bolstering the anonymity of the dark web activity. In this sense, bitcoin was specifically created to aid in the facilitation of anonymous transactions and engender blossoming of illegal activity and illegal enterprises that are ramping up productions (Krebs, 2015). Ward (2014) explains that it is almost impossible to track users' activities back to illegal sites while using bitcoin. Like most markets, it needs a private key to be verified before its use, furthering the anonymity and secrecy of these markets.

The dark web plays a significant role in allowing users a stable and consistent presence online without endangering their real life identities. While the surface web is also used for illicit activity with individuals selling illegal products and services on Facebook or alternative popular forums, these more conspicuous endeavours are routinely shut down by law enforcement officials (Krebs, 2018). Whereas Finklea and Theohary (2015) state, the dark web's anonymity is beneficial to those who want a platform to freely and privately conduct illicit activity. Thus, as researchers like Jardine (2015) suggest, the dark web plays a role in creating a dilemma for policymakers, as the technology makes it difficult for law enforcement to bring down illicit networks. It has been suggested that the ecosystem of illegal markets and enterprises are highly unpredictable when illicit content or facilitating illicit transactions vanish on a regular basis. New sites are continuously emerging every day and are primarily being used for

the purpose of distributing illicit products and goods (Owenson, Cortes & Lewman, 2018).

Existing Understanding of the Dark Web

In recent years, the darknet has become one of the most discussed topics in cybercrime based on the increase of literature, and research studies. Current academic studies accentuate the fact that the darkness' anonymous nature has increased criminal activity especially to the movement of illicit substances and narcotics. It has become a type of haven for criminals to freely conduct a range of criminal activities precisely because they are granted the ability to remain anonymous (Bigham, 2015). Technological advances and safety measures employed in this virtual space give these individuals the best possible opportunity to conduct their operations freely. Consequently, both the dark web and its associated individual marketplaces have flourished as a result of networking practices, enhanced privacy, and increased security.

The reality is that the Internet is continually evolving and new complex systems of integration and communication are continually evolving and emerging. The dark web is currently understood by academics and law enforcement officials as a hyper-private environment increasingly prevalent within the cyber world (Thomas et al., 2020). As the popularity of the network has increased, so has its usage which ranges from the hosting of expanded black markets and whistleblowing websites, to the organization of underground activist safe havens. In addition, the dark web has been viewed as a place that continues to embrace a libertarian, hack ethos, which supplements users freedom to operate and experiment online (Thomas et al., 2020). As, Thomas et al. (2020) describes, individuals who are active on the dark web use every possible measure, from technological to behavioural, to minimize (or eliminate) their digital footprints.

The dark web is increasingly viewed as the most popular and central space for emerging cybercrime and excessive freedom. The Internet's scale is immense, and many

feel the dark web is at its centre. The darknet has become a haven for regulatory evasion, crime, and national security threats (Rudesil, Caverlee & Sui, 2015). The dark web has been characterized as a network that is rapidly growing. Advances in secure/anonymous web hosting services, cryptocurrency/dark wallet, and the development of crimeware further contribute to the growth of the darknet (Rudesill et al., 2015). In particular, markets for hacking programs, cybercrime tools, and stolen data have continued to grow with no signs of slowing down. The overall understanding from law enforcement, policymakers, and researchers is that the dark web offers new economic, social, and political ecosystems that are used to safely go beyond the laws, regulations, and government oversights (Rudesill et ai., 2015).

Approaches to Studying the Dark Web

Academics who focus on this topic tend to highlight the dark web's anonymous nature and its use to facilitate criminal activities by remaining hidden to conduct criminal operations. The focus has been on illuminating exactly how individuals who use the dark web can conduct activities with little risk of being detected. For example, Beshiri and Susuri (2019) conducted a study to understand how anonymity is essential within the dark web. They found that encryption tunnelling is the main way users stay anonymous and is an essential technique to protect their identity, operations and activities. Ultimately, the platform maintains a steady participation rate due to its ephemeral nature and provisions of anonymity (Bernstein et al., 2011).

Previous criminological research appears to have heightened the perception that the darknet undertakes a range of criminal activities, such as the anonymous trading of illegal goods (e.g. drugs) via cryptocurrencies (Mihnea, Wang & Jung, 2019). Previous research has stressed the importance and essentiality of the exchanging and networking of illicit goods with the Tor browser. Most projects have focused on how criminal activities have been advanced through the dark web's technical aspects and routing systems (Qiang et al., 2014). Hayes et al. (2018) explain that researchers have looked specifically at Silk

Road's success and how this particular platform has prompted the growth of many other marketplaces. The Silk Road is commonly conceptualized as the blueprint to modern encrypted markets to successfully run services and create an extensive ecosystem to operate and distribute illicit products between buyers and sellers (Soska, 2015). The emergence of pseudonymous online currencies as payment has also been identified as an additional way that users obtain anonymity on the dark web. Encrypted currency is an example of additionally anonymity for users that allows exchanges without the immediate traceability that conventional payment systems require (wire transfers or credit card payments) (Soska & Christin, 2015). Acuisti, Brandimarte and Loewenstein (2015) refer to the increased anonymity as a privacy paradox of how it is good for individuals who want to use it for illicit activity, but creates massive challenges and issues for law enforcement and government officials. This advanced safeguarding privacy is viable at an individual, consumer, and market level.

The anonymous encryption is underpinned as the perceived advantage of the using the dark web for illicit purposes. Currently, these underground networks are primarily being used to move illegal goods and services by using the technological advancements to move, transfer, and pay for illicit products secretly. Rudesil et al. (2015) found that the dark web has engendered a fundamental shift in the criminal underground that is enabling worldwide access and distribution of products and services. The shift has been viewed as an exacerbated the problem of both drug and human trafficking, hacking, murder, and other pervasive illicit services (Rudesil et al., 2015). New criminal marketplaces have continued to crop up and develop a solid foundation of security, trust, and financing. Those who are selling illicit products such as drugs, weapons do not just reply on one site, as they drive to make their presence known across multiple sources and markets. This ensures that not only their names are out there to potential buyers, but also that if one marketplace get shut down, they will be able to continue to operate on alternative platforms.

Horton-Eddison and Di Cristofaro (2017), stated how these markets have become a serious concern to law enforcement agencies worldwide. Studies on cybercrime have looked into focusing the impact on law enforcements ability to police crimes associated with the dark web and illegal activity. Commonly looked into has been on law enforcements lacking the appropriate knowledge and understanding of the dark web and have struggled due to the lack of experience conducting effective investigations and prosecutions of criminals using these illicit spaces (Shillitio, 2019). Moses (2011), describes the most common difficulty is the regulations of technology, subsequent failure of law enforcement, and policymakers to keep up with these related technological advancements that are used to conduct illegal operations.

Given the lack of definitive quantitative data, law enforcement agencies are expected to act without comprehensive information regarding both what works currently, and what is required moving forward to address the challenges the dark web presents (Goodison et al., 2019). According to Goodison et al. (2019) those who have studied issues of law enforcement practices find that a relative lack of experience with investigatory techniques for dark web related crimes has made it difficult for law enforcement officials to build a solid criminal case against potential offenders. Current scholars like Horton-Eddison and Di Cristofaro (2017) have focused on the notion that the shift comes to online transactions has necessitated an alteration of the techniques and strategies employed by law enforcement actors. Contemporary literature has concluded that recognizing when a more traditional crime, such as drug trafficking, relies on the dark web or related technologies can be difficult. Thus, failing to acknowledge this connection risks missing investigative leads that could not only clear single cases but also disrupt larger-scale criminal enterprises (Goodison et al., 2019).

The principal challenge that various researchers cite when studying the challenges facing law enforcement and government agencies is that posed by anonymity. Anonymity makes the dark web an exceedingly difficult platform to understand and counteract.

Martin (2014) describes that while the dark web's provision of underground networking makes it easier for individuals to conduct illicit activity, it simultaneously makes it more challenging for counteracting forces to combat criminality. Identities in particular are heavily obscured on the dark web, as "buyers and vendors can use crypto-markets to interact instantly, directly, freely, and safely, without requiring any form of introduction or 'vetting'" (Paoli et al., 2017, p. 69). The dark web provides users with a high degree of anonymity to engage in the transaction of illicit goods while evading detection by law enforcement. Studies of anonymity throughout the current literature illustrate how the dark web can be accessed by a wide variety of users with relative ease, providing vendors with instant access to global audiences (Finklea, 2017). Basic Internet literacy, a computer, and access to the Internet are enough for any sufficiently motivated individual to begin supplying or purchasing illicit goods via the dark web (Goodison et al., 2019). The comprehensive study of anonymity, cryptocurrency, and encryption tunnelling with search engines like Tor have been the primary approach to studying the dark web.

Current Scope of Dark Web Research

Much of the conventional scope of dark web research has focused on the descriptive and technical side of movement of products, automated content analysis, and encryption algorithms. More recently, analyses have looked into the interests of marketplaces – including the preeminent Silk Road – that are embedded within the dark web. A practical method that has been conducted is the use of ethnographic analysis, where research explores the cultural phenomena from the point of view of the subject of the study in the analysis of markets (Gehl, 2009). The ethnographic work has mainly been directed at markets and not at other sites, including forums and social networking (Gehl, 2014). Moreover, most of the attention in this regard is paid to Tor Hidden Services, far less to I2P, Freenet, or newer systems such as Zeronet.

A large portion of current literature on the dark web has focused on the technical infrastructure of these virtual markets. As, Barrett and Maddox (2016) note that conducting digital ethnography in the dark web develops discussions on how these digital networks and markets work. Mculuhan (2016) further explains that using the dark web creates engagements in extensive research and discussion on anonymizing networks, cryptography, operations, web hosting, and browsing software. This is not to say that research has not dived into other discourses of the dark web, but a vast majority has focused on various technical discourses. As Holt (2017) explains much will explore these specialized discourses by using these tools to explore the darknet to understand how they operate and how the technology is used to move products.

Cybercrime research has mostly focused on analyzing how activities are committed and traditionally could be tracked within traditional search engines. A large portion of works have been on understanding how hidden websites within these private networks are accessed through specific software. Holt (2017) states that increasingly current research has been related to distributing the network analysis and Tor that allows users to become anonymous when using these spaces. Various research has conducted in-depth analysis and found that enhancements in search engine routing systems enable the dark web to be used for illicit purposes.

Alongside technical approaches like traffic analysis, researchers like Dolliver and Kenny (2016) or Moore and Rid (2016) use the web crawling technique to develop an understanding of hidden Tor websites. Web crawling and traffic analysis are typical in dark web research, as they constitute useful frameworks through which to explore the technical structures and advancement of darknet sites. A web crawler, sometimes called a spider or spiderbot are often known as shortened Internet bots that systematically browse the cyberspace to collect search engines for the purpose of web indexing (Holt, 2017). The web crawlers are used as an automated scraping methodology to help analyze dark web marketplaces. An analysis of the scraped data provided the basis for a subsequent

investigation of suspected criminals (illicit vendors) (Hayes et al., 2018). The results are used to demonstrate the efficacy of the proposed analytical framework for automating data collection and making that collection process more accessible to dark web marketplace investigators (Hayes et al., 2018). Where, traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns of communication (Holt, 2017). These types of research methodologies are known to be useful, as a study conducted by Owen & Savage (2016), analyzing 40 onion relays found approximately 80,000 hidden markets in the span of 6 months. Web crawlers and traffic analysis are seen as extremely popular within the scope of cyber research, as they both can result in valuable findings. Web crawlers or traffic analysis are also viewed as potent analytical tool by which to successfully locate and extract data on various dark web markets and their linkages to the traditional Internet.

Much of the current research on the dark web has been on the focus on how users mainly gain access and how it is predominantly accessed through the Tors search engine. As a result, the study of the dark web looks at the use of Tor and describe how the application creates more traffic and encryption to increase privacy of users identities (Dingledine et al., 2004). Furthermore, currently their has been a focus on how accessible these services and markets are when using tools like Tor and how other equivalent technologies also allow users to access websites sharing the onion domain (Goodison et al., 2019). Generally, research will draw on similar conclusions on the use of browser engines, specifically Tor for the benefit of gaining access to forums, markets and other hidden websites. The current focus has been on the dark web as the network that provides an environment where criminal activity flourishes. It has been found that the operations and activities range from trading illegal goods to hacking and stealing of personal data (Buxton and Bingham, 2015).

Current Research on Illicit Marketplaces

The development of illicit online marketplaces is a relatively novel phenomenon. These new illicit marketplaces have garnered substantial attention from various outlets, including law enforcement, policy agencies, and the media. The emergence of Silk Road in 2011 was most notably captured by a worldwide audience, as media attention and articles quickly documented emergence of these illicit spaces (Martin, 2014). This attention also served as the basis of newfound concern as the emergence of these spaces and found to create major panic and potential dangers. According to Moses (2012), these dangers are associated with how these new virtual markets and spaces could lead to surprise and alarm from police forces already struggling to enforce drug trafficking laws. Ultimately, these concerns have motivated authorities to express greater interest in the dark web and virtual markers, with discussions emerging on how to enforce regulations within the US Congress (Hammersly, 2012).

In academic circles, the study of illicit marketplaces has grown significantly. These virtual marketplaces within the dark web operate like more mainstream outlets like eBay, but are used for the movement of illegal goods, and permit users to trade and access a range of illicit services. These marketplaces are further differentiated by the fact that they can only be accessed through their specific ".onion" address (Tor project, 2019). Afilipoaie and Shortis (2015) found that users can provide feedback on products and sellers while using an escrow system that protects both buyers and sellers from potential scams. Even after Silk Road's closure, new markets continued to pop up as these online covert marketplaces continued to expand operations. Soska and Christin (2015) estimate that the entire darknet marketplace ecosystem generated between $150 and $180 million in revenue annually. Scholars characterize the rise in darknet markets as a demonstration of the resilience of these anonymous online ecosystems, which continue to grow yearly in spite of law enforcement agencies' counteractive efforts.

Illicit marketplaces have developed economies that supplement traditional street corner drug markets, firearms and illegal sex trades. Cromwell and Olson (2004), generated a substantive insight into the impact that virtual online markets have on traditional illicit markets. For example, online vendors now have the opportunity to sell anything, as they can offer stolen information, malicious software, illicit drugs, counterfeit products, and various other illicit services through Tor hosted sites and underground forums (Holt & Bossler, 2015). Hidden markets that use the tor encryption have been seen to create a substantial advantage in protecting identity and further operations that were not presented in traditional operations (Holt, 2017).

Various academics have attempted to use Silk Road as a case study to explore marketplace operations. Many studies have attempted to quantify the growth of user memberships to explore how these virtual encrypted marketplace spaces have grown in popularity and success (Bradbury, 2014). For example, Soska and Christian (2015), studied the growth of virtual underground markets by analyzing the organizational makeup, operations of venders and sellers, and security practices of 16 different markets. Using Silk Road as a starting point, evaluations of illicit marketplaces tend to outline the relative function and usage rate of alternative platforms. Thus, much focus has been on how new online markets have followed Silk Road's footsteps and advance the sale of illicit goods and services.

A substantial amount of research is dedicated to comparing traditional black markets and illicit online marketplaces have also been a significant focus. These online markets have been viewed to resemble the traditional black marketplaces (Pace, 2016). Pace (2016) explains that as opposed to traditional markets, the illicit online marketplaces are free from economic regulations. These markets are unique and do not feature face-to-face interactions because they are oriented towards maintaining user anonymity (Pace, 2016). However, despite the fact that these markets prioritize anonymity, they remain committed to protecting their users from fraud and exploitation. As Ulbricht (2012) notes,

these marketplaces employ a reputation system, where clients rate vendors on the basis of the quality of their goods, shipping times, and overall customer service. All client feedback is done at the vendor level, just as is the case on Amazon or eBay, where buyers can leave feedback or reviews on their experience or the quality of the product. While the feedback mechanism reduces a customer's risk of being exploited during a transaction, the use of cryptocurrency increases their relative sense of safety (Van Hout & Bingham, 2013). Therefore a central theme by academics that has been explored is the reputation system and the central importance of functionality in this markets and how if these are effective then the entire market can run smoothly (Pace, 2016).

The growth of markets has also been a focus by cybercrime research as a fundamental shift in the illicit underground economy (Sui et al., 2015). The growth of these markets have been viewed as a way to easily access illicit products worldwide with secure, fast delivery. This has lead to an international supply chain of goods and services of illegal distribution of firearms, drugs, and fraud (Rudesil et al. (2015). In traditional senses, many illicit operations are conducted in a covert manner. Conventional drug markets have evolved from 'open' into 'closed' entities, with dealers transacting only with known customers, and acquiring new customers through trusted referrals (May & Hough, 2009). Current research would suggest this is the opposite in the online markets, as academics believe the dark web has reversed this opened into closed strategy because of the layered encryption and privacy. It has created this idea that vendors can now conduct business in plain sight of law enforcement or with anyone with a computer (Aldridge & Askew, 2016).

The sheer variety of services advertised on these marketplaces has underpinned researchers' fascination with exploring their underlying composition. These studies have been geared towards classifying the content available on the dark web into several categories. While these analyses have primarily focused on supply side indicators with potentially limited utility as threat metrics (Jardine, 2019), they provide a clear sense of

the types of content available on the Tor-hosted markets. Biryukov et al. (2014) exploited deficiencies in the Tor software to collect the onion addresses of 39,824 hidden services and adopted an automated approach to classifying them into 18 categories. Similarly, Owen and Savage (2016) examined the dark web's technical side, finding not only that most services were running on Apache Web servers, but that services related to the drug trade made up 15 percent of their dataset, followed by fraud sites (nine percent) and child abuse (two percent).

To create a more detailed picture of the marketplace's content, Al Nabki, et al. (2017) increased the number of possible categories for the classification of hidden services. They manually divided 7,931 hidden services into 26 categories, of which eight contained illegal content. They found that TDIDF (or term frequency-inverse document frequency), along with logistic regression, were the most accurate methods of classifying illegal activities. Collectively, these research studies exemplify the efforts to uncover hidden services that demonstrate that illegal content is available for purchase within these illicit marketplaces. Efforts to maintain some record — through practices like reindexing — of the content featured on dark web sites are undermined by the frequent change in the hidden networks because of security reasons, dross attacks or maintenance periods. Current research in this realm is predominantly oriented towards describing the composition of these hidden markers hosted on the Tor dark Web.

As a whole, the current literature on the dark web and illicit online markets tends to focus primarily on descriptive and technical explanations, where the emphasis has largely been on the distribution of products, market operations, and their impact on criminality (Holt, 2016). It is evident from the literature review how research on the dark web has not taken a deep dive into the impact on individual behaviour or the significance of its use for illicit and criminal activity. This study aims to fit into and contribute to the field by providing a more theoretical overview and exploring the impact that the dark web has on delinquent behaviour. Utilizing the interactional theory in this analysis aims to synthesize new

theoretical ideas as well as to present a new perspective on the dark web and its impact on illicit activities and behaviours.

## Chapter 3: Theoretical Framework

This study is designed to contribute to the research on the dark web by building a theoretical framework that analyzes how the dark web impacts deviance and criminal behaviour. The objective of this study is to contribute to the field by providing not only a theoretical overview of the dark web but also a foundation for an integrated theoretical approach to develop an understanding of the dark web marketplaces, illegal tool-kits, and virtual communities, as well as their connections with criminal activity. This study aims to determine the theoretical approach and adopt a current criminological theory that can account for the dark web as a marketplace, illegal tool-kit, and community affecting delinquent behaviour and its connection to criminal involvement.

### The Interactional Theory

The ever-increasing popularity of the dark web has effectively made it necessary for the research to expand theoretical analyses detailing how these virtual spaces advance delinquent behaviour. To this end, this paper incorporates particular tenets of Thornberry's (1987) interactional theory to explore the dark web's various uses as a marketplace, illegal tool-kit, and virtual community. Thornberry's interactional theory is oriented towards evaluating the effects of both human behaviour through social interaction, and the interactive processes affecting one's potential engagement in delinquent behaviour (Thornberry, 1987). Delinquent behaviour is viewed as an informal network affected by social factors and their developmental effects, which combine to focus on social control and social learning being a focal point in the developmental framework of emerging individual delinquent behaviour.

Origins of the Interactional Theory

Theorist Thomas Thornberry developed the interactional theory in 1987, which combined not only facets of Hirschi's (1969) social control and Akers (1985) social learning theories, but additionally incorporated elements of Elliot's (1983 and 1985) integration models. Hirschi's (1969) social control theory suggested that delinquent behaviour was a direct consequence of an individual's bond to society being weakened or broken. In comparison, Akers (1985) explained that delinquent behaviour results from social learning processes, where people develop motivations to commit crime by leaning new behaviours, values, and attitudes by direct experiences of observing others behaviours. Most notably, the social learning and social control theories operate from a distinct foundational assumptions regarding the causes and manifestations of delinquent behaviour. Social learning assumes that humans can commit deviance or crime based on attractiveness (Hirschi, 1969). In this sense, when an individual loses control or bonds to conventional society such as parental attachments, they are more likely to engage in delinquent behaviour (Hirschi, 1969). On the other hand, Akers (1985) believes that there is no natural impulse towards deviance or crime. On his account, delinquent behaviour results from the socialization of deviant norms, values, and behaviour (Akers, 1985).

The justification in the combination of these two theories, Thornberry argued that both frameworks suffer from fundamental limitations, specifically as it pertains to their reliance on unidirectional structures as opposed to reciprocal causal systems (Thornberry, 1987). Thornberry (1987) claims that social control and social learning are non-developmental and only account for a narrow age range (Thornberry, 1987). The theories only assume causal effects through the social structure while ignoring structural positions and are viewed as incomplete (Thornberry, 1987).

The interactional theory emphasizes the reciprocal relationships between social control and social learning theory. Weak social bonds are viewed to provide individuals with an opportunity to be exposed to delinquent environments, and subsequently weaken

their bonds to society. The suggestion is that the weakening of social bonds are not a sufficient cause of ones engagement in delinquent behaviour, as a learning environment is needed for individuals to learn delinquent behaviours and uses these new opportunities of freedom to properly engage in delinquent operations and activities (Lee, Menard & Bouffard, 2013). Along with a learning environment, individuals need to also bond with imitate groups, by associating with peers who engage in delinquent behaviours to assist in the learning process of deviance (Thornberry, 1987). When individuals have diminished bonds to the conventional world, with no commitments to school or work, and weak attachments to family, it can push an individual to deviance by associations with delinquent peers, and learning environments to ultimately participate in delinquent behaviours (Thornberry & Krohn, 2005). The weakening of social bonds is framed as a process that enhances one's behavioural freedom, allowing individuals to operate themselves from outside the conventional world (Margot, 2018). Thornberry (1987) contends that one's attachments to parents, conventional values, commitment to institutions (school or job), and associations with peers are all related to the impact of emerging delinquent behaviour.

While Thornberry (1987) believes the social learning and social control theories are both fundamentally flawed, he asserts that combined, they construct an amplifying loop that explains the emerging effects and influences of individual delinquent behaviour. For, example low social control can increase the likelihood of an individual associating themselves with delinquent peers and participate in delinquent behaviours, which collectively inspire further reduction in social control (Thornberry & Krohn, 2005). The interactional theory frames deviance as a set of mutually reinforcing causal relationships. These relationships either develop over time and create trajectories towards or away from prolonged involvement in deviance and illicit behaviour (Margot, 2018).

Strengths and Limitations of the Interactional Theory

The interactional theory has been critiqued for its work on reciprocal effects on social learning and social control impacting delinquent behaviours, influences on delinquent norms and values to deviance. Criminologist Weerman (2011) explained that the idea of delinquent peer groups having a significant influence on delinquent behaviour can be addressed by alternative approaches that do not narrowly focus on associations with delinquent peers and their affects on delinquent behaviour. Cultures and life circumstances are other key dynamics or influencers of emerging delinquent behaviour that should be studied as focal points of how individuals can emerge in acts of deviance (Weerman, 2011). The belief is that delinquent behaviour should not be studied by this narrow framework and should not solely be analyzed from strengthening or weakening of social bonds, as other dynamics should be studied where variables such as life circumstances, race and social class should be considered in the research of deviance (Weerman, 2011).

Testing the interactional theory is also considered to be a particularly challenging task, especially with regards to researcher's attempts to evaluate variables of influencers of delinquent behaviour. For example, in analyzing the national youth survey, War (1993) hypothesized that delinquent behaviour is inspired and influenced by one's association with delinquent peers. The results indicated hardly any crossed-lagged reciprocal effects between peer association, delinquent beliefs, and delinquent behaviour. An alternative analysis of three waves of the national youth survey - conducted by Menard and Elliot (1994) found that the reciprocal effects of deviance only had moderated lagged effects of bonding with delinquent peers influencing individual delinquent behaviour. Furthermore, minor delinquent patterns were also found to have no real impact on delinquent peer group bonding (Menard & Elliot, 1994). Overall, the difficulty of testing the interactional theory has brought up some concerns in the framework of the effectiveness of reciprocal effects of delinquent peer association and delinquent bonds.

Thornberry (1987) purports that the interactional theory is able to explain some elements of delinquent behaviour with more effect then other influences. Some variables of emerging delinquent behaviours are useful tools by which to illuminate the reciprocal effects of attachments, commitments and behaviours, as through the Rochester Youth development study, Thornberry (1991) found that these three variables of emerging delinquent behaviours are the most useful and effective when testing the interactional theory. Studies that have previously tested the interactional theory have not adequately modelled social control and social learning variables. Specific variables will not indicate the reciprocal effects on delinquent behaviours and studying them is not conducive to exposing the reciprocal effects. Thornberry's (1987) explains that reciprocal influencers and effects of deviance are likely to result over time and should not be tested for imminent results. Delinquent behaviour is not a mere outcome of weakening social bonds or association with delinquent peers but a development that takes place over time through different developments and trajectories (Thornberry, 1989). Thus, previous tests of the interactional theory do no align with the theory's framework, as they fail to consider the possibility that delinquent behaviour develops over time and is not necessarily an immediate result of reciprocal effects of delinquent behaviour.

## Primary Tenets of the Interactional Theory

### *Reciprocal Effects on Social Control*

Thornberry (1987) suggests that delinquent behaviour occurs through processes of social interaction. These variables are part of a complying loop wherein low social control increases one's likelihood of associating with delinquent peers and engaging in delinquent behaviours. While deviance is fundamentally rooted in weakening of social bonds to conventional relationships such as families, it can increase one's propensity to engage in an array of delinquent behaviour, ranging from continued conventional action, weak institutional bonds, alcoholism, mental illness, and delinquent or criminal careers (Thornberry, 1987). The interactional theory states that delinquent behaviour leads to further reduction of influence that social controls have on an individual. The weakening

of social bonds facilitate one's exposure to delinquent environments and pro-delinquent values. The weakened bonds enable the emergence of individual influences of delinquent behaviour, values, and associations to delinquent peers. However, as individuals become enmeshed in these delinquent behaviours, their bonds to the conventional world will likely erode further (Thornberry, 1987*)*.

Thornberry (1987), illustrates that individuals typically attempt to maintain strong conventional social bonds, which manifest themselves in their attachments to parental figures, and commitment to school or work. Underpin one's internalization of pro-normative bonds, norms and values, and engagement in delinquent behaviour that is indirectly affected in two different ways. For one, belief in conventional values are reciprocally related to the commitment to institutions such as school or work, without these commitments one's attachments to conventional society will impact their individual behaviour. Secondly, adherence to traditional values such as marriage, good career or, religion can reduce the opportunity to engage in associations with peers who value deviance, and impact one's values and behaviours (Thornberry, 1989). In essence, if an individual has strong commitments to pro-normative values, their bonds to society will strengthen. Similarity, these attachments can directly impact the underlying influences of delinquent behaviour if they are not present, can impact the emergence of attachments to deviance.

The fundamental cause of deviance is motivated by an outgrowth of attenuation of social controls that moderate an individual's behaviour. Detachments to normative values grant individuals the opportunity to both be freed from moral constrains and engage in deviance. Social bonding is thus reciprocally linked to deviance, as it effects one's bonding to these behaviours by either the association with delinquent peers or valuing these behaviours greater then conventional values (Thornberry, 1987). As individuals engage more in delinquent conduct, their association with delinquent peers and bonds to the illegal underground are strengthened (Thornberry, 1987). The weakening of

conventional social bonds may be the initial cause and indirect impact of an individuals behaviour changing and associating with peers and environments that further eradicate attachments to family, school, jobs, and conventional beliefs (Thornberry, 1987). Deviance affects and influences one's behaviours, values, and attachments by increasing the association with environments and peers who continuously reinforce those delinquent beliefs which further structures individual behaviours and heightens their values to deviance more than conventional values (Thornberry, 1987).

*Reciprocal Effects on Social Learning*

The interactional theory suggests that both social learning and social control must be present in order for the opportunity to engage in delinquent behaviour to emerge. Thornberry (1987) explains that an interactive setting is required to assist in learning, performing, and reinforcing delinquent behaviours. The learning element is viewed as essential in two distinct ways, including learning through delinquent peers and internalizing delinquent values.

Individual beliefs are among the strongest lagged predictors of deviance, as if delinquent behaviour can be learned and reinforced it can develop a greater impact on one's beliefs to delinquent behaviour and further influence and maintain these values (Thornberry, 1994). The reciprocal variables of deviance indicate that the association with a group may strengthen their commitment to engaging in particular kinds of behaviour, such as drug distribution, theft, or other illicit operations. Resultantly, peer association is viewed to have a significant influence on delinquent and illicit reciprocal effects of social learning. Thornberry (1994), states that the dimensions of delinquent peer association could influence the learning of pro-delinquent behaviours through constant dimensions of communication of delinquent content and orientations. Delinquent peer groups are considered to be suitable social environments wherein individuals learn normative orientations of deviance that dilutes the fears or resistance of engaging in deviant operations, as the more individuals learn, the more they become

comfortable with participating in those delinquent activities. In turn, normative orientation can influence delinquent behaviour and more association with groups that offer support one's internalization of normative standards of behaviour. This indicates thats both the selection and influence of delinquent peer group association are active simultaneously (Baerveldt et al., 2008).

Delinquent behaviour does not simply emerge as a consequence of the weakening of social bonds, but is alternatively learned after those societal attachments are diluted. Thornberry (1987) argues that deviance is learned and reinforced in social settings. Absent these environments, delinquent behaviours or values cannot develop, as a learning interactive environment must be present, along with delinquent groups that can assist in learning and reinforcing those delinquent values. These two variables, along with delinquent behaviour itself, collectively form a mutually reinforcing causal loop that increases one's involvement in deviance over time (Thornberry, 1987).

This paper incorporates the particular tenets of Thornberry's (1987) interactional theory to explore the dark web's various uses as a marketplace, illegal tool-kit, and virtual community and how they impact delinquent behaviour. These tenets of social learning and social control will be used to analyze the interactional theory in the online setting and explore a new theoretical development on how delinquent behaviour can be accounted and influenced in the dark web. The rationale is the belief that the process of deviance could be accounted by reciprocal relations between social control and social learning variables over time in an online interactive setting. The study looks at the dark web as an interactive setting where incorporating theoretical significant measures of the interactional theory can explain how reciprocal relationships, delinquent peers, and delinquent tools impact and influence delinquent behaviours in the dark web over time, and how the marketplaces, tool-kits and communities account for these key influencers of delinquent behaviours.

## Chapter 4: Methodology

This research study utilizes the interactional theory to analyze the reciprocal effects on the tenets of social learning and social control to analyze their effects on delinquent behaviour within the dark web. In essence, Thornberry's (1987) interactional theory will be integrated into dark web to account how the marketplaces, tool-kits, and communities increase an individual's propensity to engage in delinquent behaviour. Conducting an explanatory case study of the Whitehouse market, this analysis aims to collect evidence to analyze and integrate the theoretical analysis of the dark web.

Relatively few cybercrime studies have focused on developing a theoretical framework to explain the social organization, relationships of users, and the role of social connections within online environments (Holt, 2017). This study looks to bridge the gap within the cybercrime research by creating a theoretical contribution that focuses on explaining the significance of the dark web and why it contributes to advancing and increasing exposure to individual delinquent behaviours.

### Research Framework

The framework of the study is using the exploratory case study that involves an up-close, in-depth and detailed investigation of a subject of study that helps bridge the understanding of a complex issue (Merriam, 2009). The flexibility allows researchers to tailor the design and data of their research topic and questions (Meyer, 2001). Explanatory case studies are useful mechanisms by which researchers can define their questions by the feasibility of the research procedures (Hancock & Algozzine, 2011). In seeking to answer questions of 'how' and 'why' particular phenomenon occur (Yin, 2014), the framework of the case study looks to illuminate the causal relationships underpinning both the materialization of a given event, and its influence on the alternative outcome (Hancock & Algozzine, 2011). The analytical generalization enables researchers to not only generalize their findings, but also shed light on theoretical concepts or principles that influence the phenomena under investigation (Yin, 2014).

The study uses the exploratory study to obtain information about the dark web in its real-life context (Crowe et al., 2011). The use of the exploratory case study is to gain concrete, contextual, and in-depth knowledge about the specific field of research of the dark web, and to explore the key characteristics, meanings, and implications of the topic (Crowe et al., 2011). The case study evaluates the effectiveness of an approach that utilizes the linked social learning and social control tenets to analyze the dark web's manifestations as a marketplace, illegal tool kit, and community.

The exploratory case study will offer additional insights into the gaps of dark web research. As Crowe et al. (2011) explain, case studies can help develop new theories or refine previous theories that aid in generating knowledge that potentially can account for or explain various behaviours (Ecceles, 2006). The framework uses the interactional theory to potentially provide accounted factors that promote deviance on the dark web. Thus, the exploratory case study of the Whitehouse market represents a means by which to find supporting evidence to discuss how reciprocal effects and influences on delinquent behaviours are accounted and impacted within the confines of the dark web. Additionally, it provides potential to create a new way of understanding the dark web and bridging the gap between the effects that the virtual underground have on individual delinquent behaviours.

The case study framework will allow critical events, interventions, policy developments, and program-based service reforms to be studied in detail within the dark web marketplace of the Whitehouse market. This approach is suitable for the purposes of providing insight into aspects of the online world. For example, Hayes (2018) and Chung (2008) both conducted case studies on the dark web to collect evidence for the purpose of their research studies. Hayes (2018) conducted his case study for the purpose of testing the idea of a web crawler tool that can collect data on dark web marketplaces in order to explore their primary uses. While, Chung (2008) conducted a case study to analyze Jihad

sites as a platforms for the spread of terrorist ideology & communication. As researchers, both conducted case studies in order to collect deep insight and information about the subjects they were studying in order to produce a more comprehensive study by acquiring data that could assist them in bridging the gap between a complex issue. Like for the purpose of studying the impact of delinquent behaviour on the dark web, Hayes (2018) and Chung (2008) used the case study method to stimulate new research in assisting to find new and advanced evidence to support their claims in the research field.

Research Approach

In conducting an explanatory case study of the illicit dark web Whitehouse market, this analysis seeks to explore the various manifestations of the dark web as marketplace, illegal tool-kit, and virtual community. The purpose of this study is to analyze Thornberry's (1987) interactional model of reciprocal effects on deviance and capture empirical data to account for a structural dynamic model (Boers et al., 2010). The study integrates assumptions underlying the tenets on social control and social learning to dissect technological advancements, peer influences, and corresponding values. Understanding the relationships between social learning and social control may aid in explaining how the three prongs of marketplace, illegal tool-kit, and community account for stimulate changes in individual behaviour and normative orientation. Moreover, why these three prongs of marketplace, illegal tool-kit, and community might reinforce and influence individual delinquent norms and values.

The use of the interactional theory within the theoretical analysis is a unique way of altering the direction of research on deviance that in the past could be viewed as limited. As Thornberry (1987) argued, other criminological theories tend to rely on unidirectional causal structures that represent deviance in a static rather than dynamic fashion. Developmental theories that suggest delinquent behaviour is learned and reinforced through reciprocal social processes serve as critical frameworks by which to understand the modern evolution of deviance (Elliott et al., 1985; Thornberry, 1987). The

interactional theory's reciprocal relations among social control and social learning looks at how deviance is part of this amplifying loop of weakening social bonds leads to the emergence of delinquent behaviours that at the same time continue to weaken normative bonds in this continuous loop. The impending study will be analyzing if this amplifying loop of deviance exists on the dark web or if there is any evidence that this occurs within the confines of the dark web.

Sample

During the exploratory study, the main sample will be the illicit Whitehouse market to gather data supporting the idea that the dark web marketplaces, illegal too-kits, and communities have an impact on delinquent behaviour. The Whitehouse market is classified as a more miniature marketplace than many other dark web markets, but it contains an active forum with considerable user engagement. The market is accessible only through the Tor browser, and with a valid membership. According to Yin (1994), the Whitehouse market is viewed as an appropriate sample that strives to explain the causal links to real world samples to link together the contexts and explore situations in which interventions are being evaluated with no clear set of outcomes. The strength of the case study is that the sample can be studied in its real natural settings that allow the study to create meaningful, relevant theories that can used to explain the implications and unique insight of the research and used to explain a deeper meaning (Ebneyamini & Moghadam, 2018).

The Whitehouse market forum consists of a small community of about 1000 users and is widely regarded as the most crucial part of the analysis. Online forums serve as transnational platforms for criminals to engage in criminal and illicit activities (Decary-Hetu et al., 2013). The data from the Whitehouse market will be used as a structural model of integration and explanation of reciprocal effects on delinquent behaviours on the dark web. Online forums offer many pedagogical advantages of teaching users how to operate within these spaces, while teaching how to network and create relationships with

others. In contrast, these forums' asynchronous text-based nature can encourage reflection on certain illicit behaviours and enable high-order thinking in regards to conducting illicit operations (Richards, 2009). The popularity of online forums is rooted in their ability to engage in communities about specific topics that are open for discussion and virtually cover every subject imaginable. Within this analysis, the forum is significant because it allows for an insight into the interpersonal interactions within the market, as well as how peer group associations impact behaviours associated with deviance.

Online forums hold essential data that provides researchers a way to craft a detailed narrative on underground markets that allow them to engage in users general discussions, propose questions on illicit products, provide recommendations for illicit products, and receive updates on news of the market. In observing darknet forums, Mirea et al. (2019) emphasized that these platforms enable various different types of dialogue that can serve as significant contributions to an analysis that is focussing on illicit operations, delinquent relationships, or emergence factors of delinquent behaviours.

Data Collection and Analysis

The primary method of gathering data for this study will be a content analysis and exploratory case study on the Whitehouse market. The first step in the analysis is collecting data from the Whitehouse market forum. The data was collected from the Dread forum site - which is accessible through the Tor browser - over a six-month time period, from December 2019 to May 2020. Online forums are perfect venues for illicit users to meet, network, and work together through the common interests of conducting illegal operations (Pitt & Fowler, 2005).

Along with the outlined use of Tor, a VPN was also installed as an additional precautionary measure geared towards maintaining the researcher's privacy during the data collection phase. While the Tor browser already provides its users with more privacy than it does from traditional search browsing software, a VPN was also implemented to

create additional layers of safety and protection. VPNs establish a secure connection between users and the Internet, through which all data traffic is routed through an encrypted virtual tunnel. In this way, your IP address is disguised, making its location invisible.

The data collection involved collecting from the forum posts in order to collect significant data and evidence for the purpose of the analysis. Both the initial posts and replies from the forum threads were recorded as a means of analyzing user interactions and discerning their significance to emerging delinquent behaviours. This sample was gathered using a purposive sampling strategy widely used in qualitative research when the goal is to identify cases with significant and useful information to incorporate into the research (Palinkas et al. 2015). The purpose of this is to select data from the forum in a way that enables the interactional theory's tenets to be included in the breakdown analysis of the marketplace, illegal tool-kit, and community impacting delinquent behaviour on the dark web. As a result, the approach not only helps prevent the accumulation of irrelevant data, but also allows the research of the marketplace, illegal tool-kit, and community to narrow the data set from over 1000 forum posts to only 243, and thus provide the research with a more refined sample to examine in greater detail.

It is the goal of this paper to gather the most relevant and useful information that will support the use of the interactional theory to explain the ways that the dark web can account for  a marketplace, toolkit, and community impacting delinquent behaviour. The Whitehouse forum contains a blend of threads related to questions, reviews, and general discussions on drugs, vendors, and the underground market. Tor and the market itself are both secure platforms, and established privacy measures ensured that each thread could not be downloaded or copied and pasted into another document. Consequently, forum posts were recorded using the Mac snipping tool to screen capture image files of forum posts and store them depending on their fit within the analysis.

As soon as data collection was complete, it was separated into different categories, and the data could be narrowed down by eliminating data that were deemed irrelevant for the analysis (Crowe et al., 2011). After reviewing the collected data, it was broken down into sub-categories relating to the marketplace, illegal toolkit, and community categories. In summary, the data was distributed to the following categories: market features, market rules, vendors, product inquiry, reviews, questions, tips/ recommendations, market changes, discussion, community warnings, news, vendors/ review, and products listed.

The coding scheme incorporated themes that focused on data that could be viewed in the contexts of the dark web in three distinct ways that could be later analyzed and explored on their impact of delinquent behaviour through the interactional theory's theoretical explanation. As this study adopts an inductive approach to content analysis, the coding strategy has been derived from the data itself. This means that the codes utilized were determined during the content analysis and constantly refined. This ultimately led to the crystallization of three main codes: (a) marketplace, (b) illegal tool-kit, and (c) community.

In the traditional study of the dark web, data collected from markets or forums have been used to analyze the dark web in a quantitative approach. Research studies with quantitative elements have primarily collected data for the purpose of analyzing and drawing conclusions about the research topic, as the data is predominantly used to test hypotheses (Albers, 2017). A quantitative analysis seeks to identify underlying trends, patterns, and relationships that can be used to interpret the context of the study (Albers, 2017). Due to this, quantitative studies are carried out through the use of statistical tests to draw valid conclusions from the data and to use the data to gain a deeper understanding of the research (Albers, 2017). Generally, dark web researchers conduct more quantitative studies, with web crawlers collecting data from forum postings, darknet forums collecting and analyzing data to find out why the dark web is heavily used for

illicit transactions, especially in the movement of drugs and illegal products. Quantitative research is a common and useful methodology for studying the dark web, but it is neither necessary nor required for this study, since the emphasis is on exploring how the interactional theory can account for the impact of delinquent behaviour.

Along with quantitative, hybrid research approaches have been used in previous research in the studying of online licit markets and the dark web. In the past 25 years, mixed methods and hybrid approaches have grown in popularity (Creswell, 2011). The incorporation of practical hybrid techniques into research offers opportunities to modify existing tools or develop new ones that are tailored to information collection as well as theory building (Mason, 2006). As, Bazeley (2018) explains mixed methods are used when the research inherently mixes strategies in which the methodology “demands” a combination of quantitative and qualitative data. Moreover, it also includes research that begins with qualitative data analysis, but then uses (usually exploratory) mathematic techniques to summarize, record, and present the data (Bazeley, 2018). In hybrid research, data are analyzed in combination with complementary techniques, or analysis unified through the application of discourse analysis. In practice, hybrid procedures are inherent to almost all data, and methods used to gather, display, and interpret social networks largely qualitative in nature, yet they rely on statistical analyses that are presented with visual representations and interpretive comments (Bazeley, 2018). Dark web research will use this hybrid approaches, such as Lilou et. al (2017), who conducted a hybrid approach to focus on web crawlers to enable automatic discovery of dark web resources and navigate the web link structure to find significance in why the dark web is commonly used for illicit operations. This study's focus is not necessarily on combining qualitative and quantitative research, but on building a theory and exploring how the interactional theory can be used to help understand how dark web marketplaces, illegal toolkits, and virtual communities may contribute to delinquent behaviour.

Despite the fact that both quantitative and hybrid/mixed approaches can be employed not only in traditional research but also in dark web research, the qualitative research approach is deemed the best technique for this study. By using qualitative methods, the researchers are able to construct narratives within each of their studies and create concepts and beliefs based upon those narratives. For qualitative researchers, paradigms are important; they help guide their research and are seen as the backbone of qualitative research, as they shape realities and determine how the researcher unravels them within their study. Qualitative research enables us to make sense of reality, and develop explanatory models and theories through which to describe the social world. It represents the primary mechanism by which the theoretical foundations of various social sciences may be constructed or be re-examined (Morse & Fields, 1996). An important benefit of developing this research about the dark web through a qualitative perspective is the ability to explore a new way of thinking about delinquent behaviour and how it impacts the dark web. Specifically, studying the dark web from a theoretical perspective is more appropriate because qualitative methods aim at generating an understanding of a phenomenon by observing it (Morse & Fields, 1996). Qualitative research provides the study the opportunity to explore the impact of the dark web when focusing on emerging online delinquent behaviours and how developing a theoretical foundation to explain the phenomenon could help to create a better understanding of these spaces and their significance in deviance or potentially allow a new way to construct theoretical studies on the impact of the dark web.

In terms of analytical strategy, this research study will explore how the virtual market, illegal-tool-kit, and communities of the dark web might be able to account for delinquent behaviour through reciprocal relationships between social control and social learning principles within the interactional theory. The purpose is to analyze how markets, illegal tool-kits, and communities account for casual associations with delinquent peer groups, advancements of technology, and acceptance of pro-delinquent norms as influencers of deviance on the dark web. Additionally, the study will aid in

interpreting the reciprocal effects on social bonding and social control on delinquent behaviour within the dark web, and how they are influenced and effected by the three concepts of marketplace, illegal toolkit, and community.

The reciprocal relationship between social control and social learning manifests itself in the formation of an amplifying loop that accounts for the increase of delinquent behaviour on the dark web. The purpose of the exploratory case study on the Whitehouse market is to find evidence that can account how the tenets on social learning and social control impact reciprocal effects on deviance when looking at the three man sectors of the dark web. It explores the possibility that the marketplace, illegal tool-kit, and community are dark web sectors in which individuals are most likely to associate with delinquent peers and to engage in delinquent activity. Through examining the dark web in these three distinct ways, the study demonstrates how the dark web can be used to foster environments that allow delinquent users to learn, reinforce, and perform delinquent acts, as well as to bond with pro-delinquent values. Within this study, the research strategy is to explore how dark marketplaces, illegal tool-kits, and online communities can position themselves as platforms that facilitate crime. Using Thornberry's (1987) interactional theory, the idea of marketplaces, illegal toolkits, and communities will be explored as the ways within the dark web that create the freedom and opportunity for delinquent behaviour and strengthening of pro-delinquent bonds.

## Guiding Concepts

### *Marketplace*

An illicit marketplace is considered a haven for criminals to undertake a range of criminal activities (Bellaby, 2018). The anonymity of these markets through encrypted software like Tor allow users to remain anonymous online, where their identities and activities are protected through layered encryption (Bellably, 2018). Anonymous online markets use these technological tools to allow buyers and sellers to hide their identities

and safely conduct illicit operations (Du, 2020). As a result, many prohibited goods, such as drugs and private data, have become leading commodities in such underground markets. In addition to this new trend of pronounced anonymity, the Internet is also a venue where individuals can communicate via encrypted transmissions to increase privacy measures, allowing them to communicate more easily and quickly with others. As a result of the Internet-mediated communication revolution, not only can communication improve, but also there is a greater potential for networking with other fellow peers within the marketplaces. Due to the advanced Internet-mediated nature of communication, there is a greater chance that users will network, communicate, and associate with their delinquent peers to engage in illicit activities on the dark web. Also, marketplaces also function as echo chambers, where common beliefs within a market are amplified by communication and repetition inside a closed, insulated system, thereby increasing peer attachments and their influence to delinquent peers through self-enforcement.

The elements of provision of an anonymous environment, use of Internet-mediated communication, and echo chambers will be explored within the marketplace to see if the interactional theory can account for them being an impact on delinquent behaviour within the dark web. At the same time, to explore external control dynamics such as laws are being reduced so users will be more likely to hold on to delinquent values, and continue to engage in delinquent behaviour. This hypothesis implies that the three elements of the marketplace being explored can give individuals more opportunities to engage in illicit activities, and may also increase distinct pro-delinquent values. These elements can potentially facilitate the weakening of one's social constraints to the conventional world, as the anonymous environment may increase opportunity and choices to engage in delinquent behaviours, and dilute one's bonds to the conventional law-abiding world.

*Illegal Tool-Kit*

Two dynamics in particular will be highlighted in the exploration of the illegal tool-kits within the dark web impacting reciprocal effects on social learning and social control impacting individual delinquent behaviours. First, the dark web offers users cutting-edge technological advances that they maybe used to conduct illicit operations. Gordon et al. (2003) argue that technological advancements contribute to the emergence of delinquent behaviour because they allow users to encrypt, store, and transmit information without fear of detection by law enforcement. Individuals can learn and advance their criminal operations using advanced technology within the dark web, which allows for freedom and opportunity to operate however they wish, as many individuals will use these advancement technologies for illicit purposes. To some extent, the primary mechanism of Tor can be seen as a technological tool that reinforces a delinquent worldview while reducing attachments to the conventional world. The tools that individuals have at their disposal on the dark web become an active part of the developmental process and the person's ultimate repertoire. Secondly, online delinquent associations can assist in users learning, and reinforcing delinquent behaviours and values. Thornberry (1987) illustrates that when individuals enter a delinquent environment, they learn delinquent behaviour from associations with delinquent peers who not only assist in learning criminal activities but also reinforce behavioural and attitude consistency in the delinquent environment. The learning from peer group associations is considered to be a vital tool-kit within dark web spaces since it helps individuals develop enterprise skills and reinforce delinquent behaviours (Gordon et al., 2003).

The assumption within this sector is that the illegal tools-kits of technological advancements and the opportunity to interact with and learn from delinquent peer groups can account within the interactional theory to have an impact on individual delinquent behaviour on the dark web. By learning illegal tool-kit behaviours and interacting with delinquent peer groups, individuals gain access to learning and committing illicit

behaviour. In essence, the dark web's illegal tool-kits are seen to impact social control and social learning reciprocal effects on delinquent behaviours.

*Community*

Using the interactional theory also will help explore how the dark web's community aspect affects reciprocal effects on social learning and social control on individual delinquent behaviour. The dark web provides more than just criminal activity, but also enables the creation of groups and social networks that can create these community-like environments (Holt, 2014). The purpose of exploring this community idea is that it fosters a sense of safety and security for those participating in illicit activity by creating structural networks oriented towards maintaining the integrity of the organization. Therefore, delinquent peer group association, values, and bonds will be examined to see how they impact reciprocal effects on delinquent behaviour. The community sector will be explored on how they are built through the strengthening of individuals' delinquent bonds and values. Without them, these dark web marketplaces could not survive, as strong bonds to deviance help create structures and systems that make it difficult for outsiders to infiltrate and destroy. The community sector will be focused on how similar interests are able to bring individuals together, how these common interests influence the structure of a community, and how similar values influence reciprocal effects on delinquent behaviour.

The idea is that community within the dark web can reinforce and further justify delinquent behaviours (Thornberry, 1987). We will emphasize the associations with peers within each of the elements in the community section, since associations with peers may result in an individual's connection to delinquent behaviour and bonds to deviance strengthening. As such, the community may be identified as a familiar social environment where social bonds are directly influenced by individual values, beliefs, and norms (Thornberry, 1987). In this way, dark web communities maybe accounted for within the interactional theory where delinquent behaviour is learned and reinforced. Over time,

one's association with delinquent peers in these online communities strengthens their adherence to delinquent values.

Limitations

By exploring how the dark web marketplace, illegal tool-kit, and community impact delinquent behaviour using the tenets on social learning and social control, the exploratory analysis will be able to better understand how delinquent behaviour is influenced by these three variables. The analysis concentrates on the impact of reciprocal effects of social bonds and social learning on delinquent behaviour as well as the causal loop between deviant peer associations and strengthening of delinquent behaviour and bonds to the dark web. Based on the Whitehouse market sample in this study, the forum displays individual-to-individual interaction through numerous comments and posts. Research focusing on the interactions within the forum and relying primarily on data collected could limit the study to account for existing pre-attachments to conventional society or individual pre-attachments to pro-delinquent behaviours outside the market. Furthermore, the data could be limited to consider or account for user engagements in the Whitehouse market lessening attachments and bonds to normative society in the amplifying loop that Thornberry (1987) describes occurs within the individual process of the interactional theory. Thus, since the Whitehouse data evidence needs to be taken at face value and since it is being examined at the individual-level engagement from the forum, the data may have limitations of not being able to take into consideration or account to the entirety of the interactional theory.

## Chapter 5: Findings

This study will examine the application of the interactional theory and how it is applicable to delinquent behaviour on the dark web when functioning as a marketplace, an illegal toolkit, and an online community.

Descriptive Overview

The descriptive findings indicated that 200 related posts from the Whitehouse market forum related to dark web functioning as a virtual community by mentioning elements relating to either to community activities or memberships to the marketplace. On the other hand, where 200 posts related to the concept of a virtual community, 165 and 111 posts addressed the concept of a marketplace, where topics ranged from the sale of illicit drugs to the usage of illegal tool-kits through anonymizing technology and peer group association. As a testament to the viability of the coding logic, despite the outlined variance, none of the categories were found to lack evidence of supporting data from the Whitehouse forum.

The analysis also displayed that certain posts were applicable to (or could be classified under) multiple categories. While 231 of the posts applied to both the marketplace and community groupings, 188 also applied to the illegal tool-kit grouping. In addition, 107 posts fell into the marketplace and illegal tool-kit categories, and 20 posts fit into all three. As a whole, a majority of the forum posts could be classified under one of the three outlined tabs: marketplace, illegal tool-kit, and community. This finding justifies the use of these three outlined categories as lenses through which determine the applicability of Thornberry's (1987) interactional theory to analyses of the dark web's impact on delinquent behaviour.

| Codes | Number of Data Sets |
|---|---|
| **Marketplace** | 165 |
| **Illegal Tool-Kit** | 111 |
| **Community** | 200 |
| **Marketplace/Illegal Tool-Kit** | 107 |
| **Marketplace/Community** | 231 |
| **Illegal Tool-Kit/Community** | 188 |
| **Marketplace/Illegal Tool-Kit/Community** | 20 |
| **Total** | 1022 |

*Table 1.Coding breakdown of analysis*

Marketplace

*The Marketplace's Provision of an Anonymous Environment*

An individual's opportunity for engaging in delinquent behaviour can be increased by the anonymizing encryption of the marketplace. These security and privacy features are viewed as significant elements that draw users to the marketplace to conduct a variety of activities and operations. As a part of the WHM platform, users are able to enjoy the anonymizing environment that adds to the drug supply chain, making it easier for consumers to acquire illicit substances. Market administrators are constantly advocating for both advancements in technology and seeking new tactics to increase user privacy. Consequently, anonymization technology is used and routinely endorsed by users who are active in the market. For example, a Whitehouse moderator posted, *"Public PGP keys-kept encrypted, messages between users (end to end encryption), messages between users and admins (end to end encryption). "Support tickets, message attachments (end to end encryption), if a user closes his account, all information related will be purged, no PGP private keys are kept on the servers, Monero private keys are kept on the servers, and main wallet is only kept offline" (Figure 1.0).* The market's users conduct a variety of

illicit operations within the market from the help of the various types of techniques and encrypted technologies available, that enables free operation. Users can take advantage of these encrypted features to carry out illicit activities to a greater extent than they could on the surface web because the dark web is the only Internet server that provides the technology to gain privacy plus warrant-proof protection without interferences. WHM officials are constantly reminding users about layered encryption tactics to protect their information they are sending and ensure their identities remain anonymous. In this sense, the WHM officials reinforce the notion that the forum's inherent anonymizing technology provides 'privacy plus' warrant-proof protection for all members.

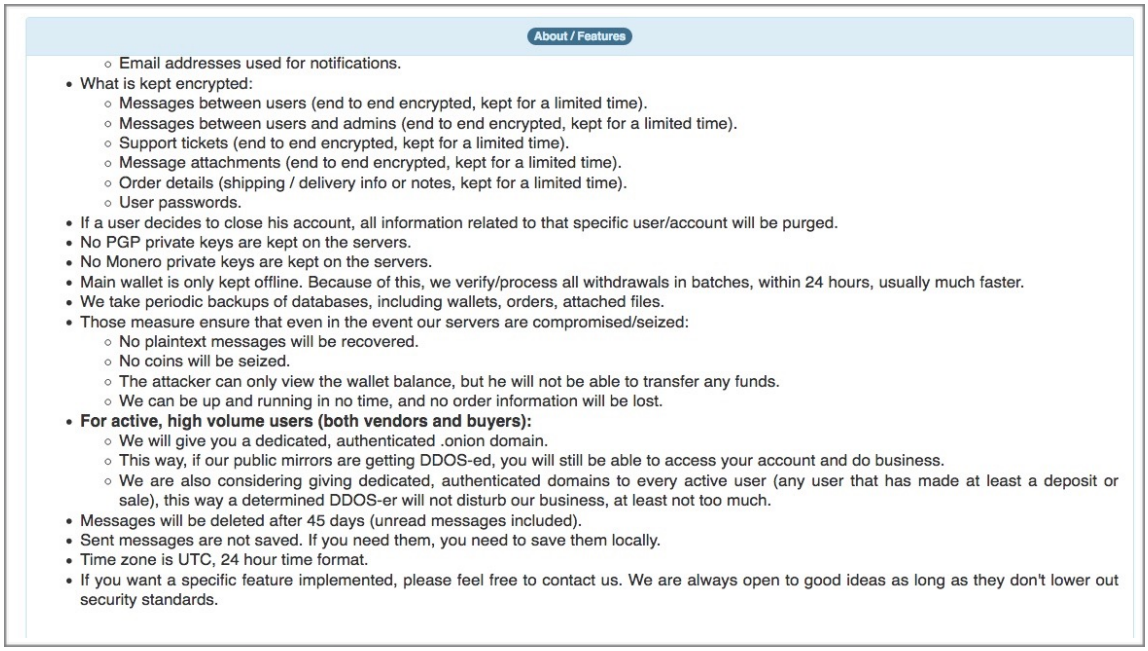


*Figure 1: Whitehouse Market About/features*

The market's administrators strive to constantly provide encrypted technologies that anonymize user's information within the market. A prominent example of this technology is the implementation of message encryption and PGP keys to hinder the ability of law enforcement agencies to collect intelligence in regard to market activity. Those in charge of the market continuously try to discover and improve new innovative novel anonymizing techniques, and disapprove others that might compromise the markets

security. For example, *market officials posted that "We have added a private jabber server for market users. The server is only reachable via Tor, and S2S is not enabled, so you can only communicate with other market users and market admins. End to End encryption is enforced, so please use either OMEMO, OTR or PGP encryption. Plaintext communication is forbidden. When you register and add your PGP key, a jabber user is automatically created for you".* Security is constantly being improved in the market, as administrative officials create reassurances for user privacy by improving and innovating new anonymized technology. As a result of these enhanced protection levels, users are allowed to engage in illicit behaviour with less concern over being discovered and exposed to external interferences. In this sense, user behaviour can be influenced by the combination of anonymity, encrypted measures, and easy access to illicit substances provided by the WHM.

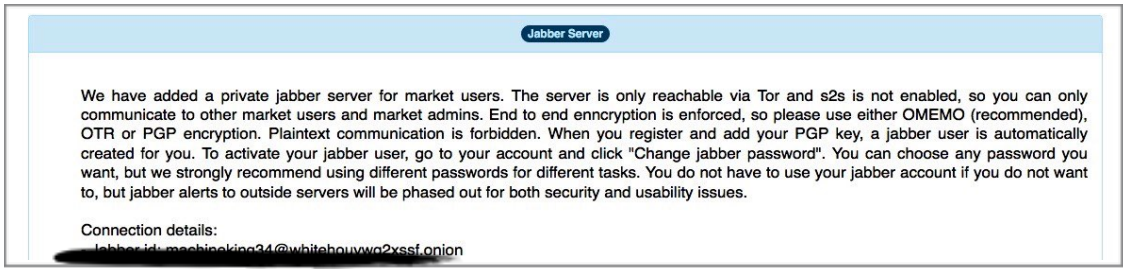


*Figure 2: Whitehouse Market Jabber Server Announcement*

The benefits and true value of anonymizing technology are evident in the WHM. Without these private and security-enhancing components present the WHM would have difficulty continuing to operate. Security is the number one priority for all user's and is ensured by the extreme measurements. For instance, users who lose their PGP key completely lose access to their accounts. PGP or 'Pretty Good Privacy' provides cryptographic privacy and authentication for data communication. A PGP key is used to sign, encrypt, and decrypt texts, e-mails, files, directories, and entire disk partitions as well as to increase security communications. By deploying PGP encryption for all transactions, and purchases of illicit products, the market ensures and maintains buyer and vendor anonymity throughout.

These virtual markets also enhance the privacy and security of user purchases by promoting the use of Monero and Bitcoin currencies. In markets where illicit goods are routinely traded and sold, cryptocurrency is the primary method of payment. Cryptocurrency is viewed as another factor that accounts for users' influence and opportunities to distribute illegal substances because it provides more security and ease to move illicit products. Forum posts reference discussions concerning both the transfer of funds to crypto and the prioritization of crypto over fiat currency. Using cryptocurrency that is verified and filed away by a decentralized system as opposed to centralized authorities can provide user's an additional layer of security to be able to engage in illicit transactions that can account for the potential increase of influence on individual's deviant behaviour.

Based on the postings, the WHM members suggest that social bonding variables can reciprocate across user discussions at different stages. By implementing strong market security mechanisms, the markets not only creates an environment that ensures anonymizing encryption for all users, but also allows free engagement in delinquent activities that could lead to a strengthening of pro-delinquent bonds to the market. Markets that have strong security mechanisms in place not only guarantee the anonymity for all users but also could theoretically prompt the increase of influences on individual delinquent behaviour. For example, a forum moderator states; "*Sales are surging. The Whitehouse market is picking up; I would recommend this site to vendors and buyers. There has been a surge of activity due to security. 100% the most secure market online right now and maybe ever"*. By providing a secure environment for free distribution of illicit products, warrant-proof spaces facilitate the easy distribution of illicit products on the market. Secure environments have the potential to influence individual delinquent attitudes and influences, as they reduce the likelihood of law enforcement officials being able to intercept and catch them conducting illegal activities. The marketplace, according to Thornberry (1987), provides an interactive setting that increases a person's chances of

engaging in delinquent behaviour and could account for strengthening their connection with delinquent norms and behaviours.

The WHM may experience a resurgence of delinquent behaviour that is exclusive to illicit marketplaces, as many of their user's previously engaged in traditional drug activities and simply transitioned onto the dark web. Vendors appear to be a mix of professional drug dealers with close ties to production and regard the online market as an additional revenue source, whereas 'newbies' previously only sold drugs to friends. Additionally, because they are typically recreational drug users themselves, buyers will often be attracted to cryptomarkets as places to buy drugs due to their perceived safety, improvement in quality, selection, and speed of delivery. The WHM offers a variety of dealers, products, quality, and prices that can entice prospective consumers to use these virtual markets to buy illicit drugs securely and quickly while avoiding the risks of procuring them through traditional means.

The WHM has a high volume of users purchasing, selling, or inquiring about illicit products, based on price, quality, and stealth shipping methods. Cocaine, marijuana, modafinil, and MDMA represent the most commonly purchased products. Many postings that use terms such as *pure, genuine*, and *top* demonstrate that drugs are of the greatest interest and are comparatively sought after for their highest quality. The interconnection between the anonymous environment and interest in illicit drugs could be exclusively present within illicit marketplaces. This could increase delinquent behaviour that is exclusive to the distribution of illicit substances by either the needs of sellers or buyers. The interactional theory may also account for the provision of anonymous markets impacting and influencing individual delinquent behaviours because of the fact only individuals with a PGP key are the ones being active, either as a vendor or customer. PGP keys can only be obtained by users who have purchased, sold, thought about, or attempted to distribute illicit substances. This may indicate that in these underground markets, participation in illicit activities and operations is increasingly dependent on the

presence of devices or gateways (Child, 2010). There is a possibility that some WHM users may already be familiar with pro-delinquent norms and behaviours before they began participating within WHM. Nevertheless, delinquent behaviour is likely to be reinforced and strengthened by the market's focus on the enforcement of anonymizing measures that ensure the ease of trade and distribution of illicit substances.

*Internet-Mediated Communication*

It is believed that the WHM's forum serves as an important element for enhancing communication within the underground network, as there is a correlation between Internet-mediated communication and illicit activities within market. User interactions in the forum suggest that users are interacting more with each other because of the advanced communication tactics available in the WHM. This platform allows members to analyze products based on quality, shipping speed, and security to determine the best purchase option. Due to this, conversations on illicit products can be more easily communicated between users and vendors, thereby increasing their association with one another. The majority of these communications are generated by ads (or listings) placed on the forum by vendors and product reviews posted by other members.

A considerable amount of discussion, reviews, and product inquiries are posted within the forum for the members, reflecting an increase in conversations and dialogue about illicit operations. Encrypted messaging benefits both buyers, vendors and admins due to the fact that messages remain secure and private throughout user conversations through the use of end to end tunnelled encryption. WHM is praised for *"their security that goes far beyond while minimizing the inconveniences of everyday use due to high security and anonymity."* By utilizing end-to-end encrypted messaging, advanced communication techniques create an increase of users' level of association with delinquent peers, while maintaining anonymizing protection so that their engagement and

affiliation are kept hidden that ultimately lead to an increase of illicit activity throughout the market.

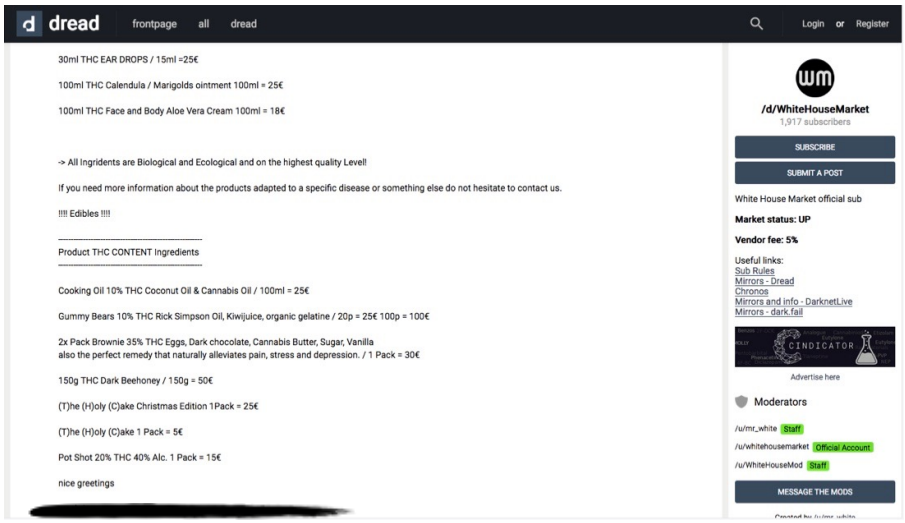


*Figure 3: Whitehouse Market Product Posting*

In addition to making it easier to deal with buyers and sellers, the market itself also increases the facilitation of the sale of illicit goods. Anonymizing technology such as, crypto-wallets, and encrypted messaging combine to make interactions between buyers and sellers on the WHM more secure than traditional means of distributing illicit products. They also make it the fastest and most efficient way to move products without attracting the attention of law enforcement. In order to conceal their activities, most WHM members regularly discuss aspects of operational security in detail, including the details of encryption (messages, PGP), escrow services, scams, and using different cryptocurrencies (Bitcoin, Monero) to complete transactions. By using these marketplaces, buyers and sellers can communicate anonymously through Internet-mediated communication tactics with other delinquent peers and can exacerbate the reciprocal effects on social control to influence delinquent behaviours through the increased opportunity to safely and privately to conduct illicit operations.

Vendors and consumers both benefit from cryptomarkets compared to traditional markets, since Internet-mediated communication protect individual conversations and make it easier for people to network and communicate. Throughout the forum, participants can find more options for drugs or vendors to purchase from, as well as to obtain better products through more secure transactions and delivery methods. Thus, thanks to enhanced services and swift communication tactics, the interactional theory could account that users develop stronger bonds with these markets because the advanced tactics of Internet-mediated communication make it easier to communicate, and distribute illicit substances without the need to endure increasingly high risks of being caught.

*Marketplaces as Echo Chambers*

As an echo chamber, dark web marketplaces can also serve as a means of perpetuating the primary purpose of the market by constantly reinforcing postings of the most discussed topics. Discussions among many users tend to revolve around the similar shared interests and values around the markets products, promotions or distribution of products. Through the increased of peer group associations, specific values, behaviours, and norms that are common throughout the market are introduced and reinforced. As a result of the analysis of the WHM, members are repeatedly discussing topics such as buying or selling illicit products, anonymizing tactics, and recommendations to conduct illicit activity safely. Moderators contribute to this type of behaviour by regularly posting features and guides that reinforce the market's core values. For example, WHM moderators will post about the idea of anonymity, noting, *"PGP signed mirror list/market statement/canary with proof of freshness, updated at least once every 72 hours. Deposit addresses are PGP encrypted and signed to deter MITM phishing. Configurable, PGP encrypted jabber/XMPP notifications for both vendors and buyers. Configurable PGP email notifications for both vendors and buyers. The use of Private Jabber serves, PGP challenge-response two-factor authentication, and messages being truly encrypted where not even moderators can see them"*. The echoing from the administrators of the market

serves as a further reinforcement of the fact that the market is mainly used for illicit exchanges of products, and reinforces the safety for participants by constantly highlighting the layers of protection that the market offers.

The WHM constitutes as an interactive setting where users echo similar shared values. There are visible elements of confirmation bias throughout, as users' decisions and posts influence the environment's values and behaviours. There is confirmation bias within these underground markets because the information commonly sought out is consistent with the beliefs of the markets users and predict the overall behaviour of the market. Particularly, users' posts reinforce the use of the market is primarily for delinquent activities, with discussions centred around the trade of illegal drugs, novel psychoactive substances, prescription drugs, and other often illegal goods and services. As opposed to being a forum that contain contentious debates or divers opinions, the discourse is instead filled with congratulatory affirmations of illicit behaviour and activities, as well as a constant repetition of some of the most tired ideas and opinions of the use of the market for illicit operations. The WHM forum posts that were analyzed provides evidence that no one advocated for its use for anything other than the sale and provision of illegal goods and services. As a result, the market is inevitably filled with like-minded individuals that reflect and reinforce the markets purpose, and distorting other perspectives. Members are influenced by each other's reactions, and their behaviour is echoed by behaviourist and normative models of deviance, intrinsic and extrinsic reinforcement, and expressive delinquent activities (Thornberry, 1987).

As market-valued behaviours are increasingly common within these underground markets, users can account for the encouragement, learning, and reinforcement of delinquent behaviour. Peers are able to associate with each other more easily as a result of the open communication and dialogue that takes place in the market. Users, moderators, and vendors who share similar values will be less likely to resist the influence, development, and amplification of those values by the association with delinquent peers.

Discussions about illicit substances and anonymizing technology create this casual system of echoing delinquent behaviours using social interactions. There are also emerging influences on reinforcing users' engagement in delinquent activities, as market officials constantly remind individuals to remain hidden, use encryption, and use cryptocurrency to conduct illegal activities. Through the influence of illicit values, the market might create an amplifying loop in which pro-delinquent norms are reinforced by informal echoing and group associations influencing deviant behaviours.

## Illegal Tool-Kits

### *Technological Advancements*

The previously outlined technological advancements seem to work as significant tool-kits within the WHM. As members who learn how to utilize the technology are able to learn, perform, and commit a variety of delinquent operations. PGP encryption and private jabber are among the examples of advanced technological tools that users are taught and use to avoid infiltration, hacking, and tracking. The market participants utilize these anonymizing mechanisms to not only enhance restrictions but also make it easier to purchase illegal substances. In addition, users often discuss encryption techniques such as tunnelled messaging and escrow to further advance the facilitation, purchasing, and sale of illicit products. Vendors will also post advertisements in order to try to entice consumers to buy their products by using advertising tactics such as the use of encryption, escrow, and stealth delivery to safely deliver products and minimize potential interceptions. Vendors who specialize exclusively in drugs are extremely common on cryptomarkets as their illegal activities are able to be expanded without the increased danger of detection.

By using the site's 'privacy plus' mechanisms, users are not as concerned about incriminating information from their past purchases and activities being stored on their accounts, since the market automatically deletes messages that mask user identities and

create barriers from incriminating evidence. If PGP keys are lost or closed, all user information is immediately wiped out, instantly increasing the level of protection against external threats of law enforcement and incriminating information. The reason behind this is that PGP keys are only generated for one per user, which serves as an authentication tool. The user must verify its authenticity before it is use and if it can't be verified then for safety protocols, it is immediately destroyed. PGP encryption is emphasized heavily by market officials, as various posts are signed with users' PGP-keys and contain strings such as "BEGIN PGP SIGNED MESSAGE" and "END PGP SIGNATURE," which likely contribute to the emphasis of anonymizing protection. Using PGP's leads to the conclusion that it further increases anonymizing protection and influences market behaviour that eventually increases chances for individuals to be involved in illicit activities and behaviours.

As an additional security measure for illicit transactions, the market utilizes a third party system to handle exchanges of cryptocurrency. The market encourages these third party cryptocurrencies exchanges and use of crypto wallets in order to maintain anonymity while conducting illicit activities and transactions. An entire section of the forum is dedicated to these third party exchanges and instructions of using crypto wallets in order for vendors and buyers to be able to freely operate and distribute illegal substances without endangering the market. Moderators emphasize that to conceal and contain the amount of illicit activity that is being conducted, cryptographic technologies are required. This is taken so seriously by some vendors that they only accept Monero, as they believe Bitcoin lacks the necessary security and privacy measures.

*Learning from Peer Association*

The WHM forum is also used for a variety of question and answer interactions that increases peer association through the use of forum postings of general and specific technical questions. The question and answer posts are heavily related to delinquent

activity, such as posts about; *"always stay in escrow*," "*reinforcement of PGP when communicating with vendors*," *pay with Monero, as it's safer*, or e*xplaining how to set up encrypted shipping addresses*." The forum posts allow both seasoned and newer members to have the opportunity to learn new tactics that could possibly influence delinquent attitudes and behaviours. The question and answer interactions build rapport with the community as well as allow for the exchanges of information, as examined posts indicate that the majority of forum questions will be answered by one or more members. As part of the forum, peer mentoring appears to be highly correlated with engagement in illicit activity, since learning new skills from peers appears to be a primary source of development of delinquent behaviours.

A similar degree of peer group interaction is also visible in the WHM, since a significant number of interactions offer user advice based on seasoned users experiences in the WHM or in other cryptomarkets. Inexperienced users are more likely to benefit from this as they have the opportunity to learn from experienced users and assist in not only learning how to operate in the market but also able to reinforce the specific behaviours that is accustomed in the marketplace. Thornberry's (1987) interactional theory can account that members learn from these interactive settings, and can help bolster individual delinquent attitudes and behaviours from the influence from the association of delinquent peer groups. Detailed analysis from forum posts referred that seasoned users are willing to assist others learn how to operate and conduct illicit activities. Those who claim to be new to the market often ask questions and specifically declare that they are "noobies" - the term refers to a new or inexperienced user. These posts usually indicate that new users – who are likely traditional drug users and vendors that transitioned onto the dark web – are motivated to engage in illegal activities, but need assistance in navigating the market and understanding features such as PGP, escrow, and crypto. As a result of interacting with experienced users, members are both more informed and strengthen their relationship with delinquent peer groups that influence their norms and beliefs.

While some moderators, vendors, or other seasoned users may be critical towards new users, many are also welcoming and see new user's as an opportunity to advance the flow of illicit goods and the overall economy of the underground market. Vendors view this more from an economical perspective as an incentive to encourage new members to purchase illicit products from them. Vendors are motivated to sell their products or services to potential new customers in order to increase their client base. Ensuring their presence with new members may allow them to gain additional new customers and increase their income. Vendors with a good reputation and an existing clientele who can vouch for them are more likely to be able to gain new customers and are keep them as returning buyers. This will not only increase the vendors clientele, but also possibly influence new buyers to continue to return, thus influencing delinquent behaviours and bonds to the market and the vendor.

Moderators also appear to be eager to help new users, since doing so expands the markets ecosystem and boosts activity levels. However, they are still known to be critical and one of the first to criticize new members with comments like "how do you not understand?" or "follow the rules or get out" or "losing PGP key means account lost, you knew the risks." Moderators are more critical to new users because they represent greater threats to the security of the market and are less likely to know how to safely and securely operate within the market. Non-vendor users are also motivated to associate and help new users, but are critical to those new users who are coming from other illicit markets. This seems to be because users expect that those types of newer members should know how to operate in an illicit marketplace. Members seem less motivated to associate with those types of new members who "complain about WHM" and even reply with statements like, "then go back to where you came from". User efforts and administrative decisions seem to be driving the effort to establish long-lasting online communities that function as consistent and coherent digital societies with identifiable membership bodies, technical structures, and cultures. Those who reply to posts indicate that they are willing to teach new users and reinforce the values and behaviours of experienced users.

Throughout, peer association also occurs, where users provide detailed technical advice to others on a variety of topics, including hacking, security, and using anonymizing techniques. During the on boarding process, moderators and seasoned users contribute to deep technical knowledge and detailed guides to help new users. A prime example of these assisted guides is the posting of a step-by-step guide on how to transfer and pay in cryptocurrency. The figure below shows a 6-step process users go through in order to exchange currency for cryptocurrency. Guides posted by users enable illegal activity to be learned and performed efficiently. It is positively correlated with how interactional continuity emerges in social interactions with peers who may reinforce personal behaviour patterns.

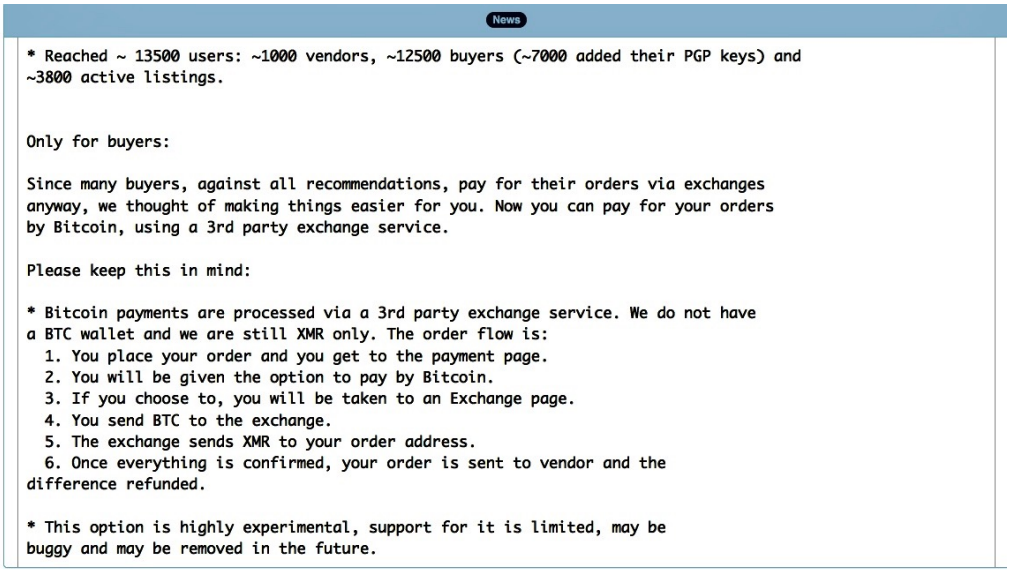


*Figure 4: Whitehouse Market News, Steps for purchasing Bitcoin*

## Community

*Common Interests Strengthening Bonds*

A wide variety of individuals participate in the WHM because they are interested in illicit drugs and substances. During the forum's network assortativity, nodes of association of high- and low-associations are connected by users' desire to buy or sell illicit products. The WHM is characterized by close relations and complex social relationships that are illustrated by its members' routine participation in regular discussions. Simultaneously, the forum's decidedly closed and private nature allows for both users to be open in sharing their interests and for online communities to be more inclusive (Kozinets, 2010).

WHM indicates that multiple perspectives, normative orientations, as well as behavioural patterns, are prevalent between peers, and are impacted by reciprocal effects on social learning and social control over delinquent behaviour. Members tend to concentrate mainly on market-related conversations and discussions regarding safety measurements to facilitate and execute delinquent operations such as selling or buying illicit substances, or communicating with vendors about the availability of certain illicit products. It appears to be a highly knit community united around members with specific interest in delinquent activity.

As a result of the anonymizing technology that the market offers, there is a higher degree of posting and replying between users. The suggestion is that the platforms enable more open and intimate conversations between users seeking advice and advanced discussion revolving around illicit topics. The increased protection offered by encrypted technologies facilitates greater ease of seeking information and exchanging practices in open spaces. In Figure 5.0 you can see an example of how the forum is being used to share practices and make the market more appealing to people due to the availability of

products, the ease of committing illicit transactions, and the ability to communicate more easily with vendors or other members.

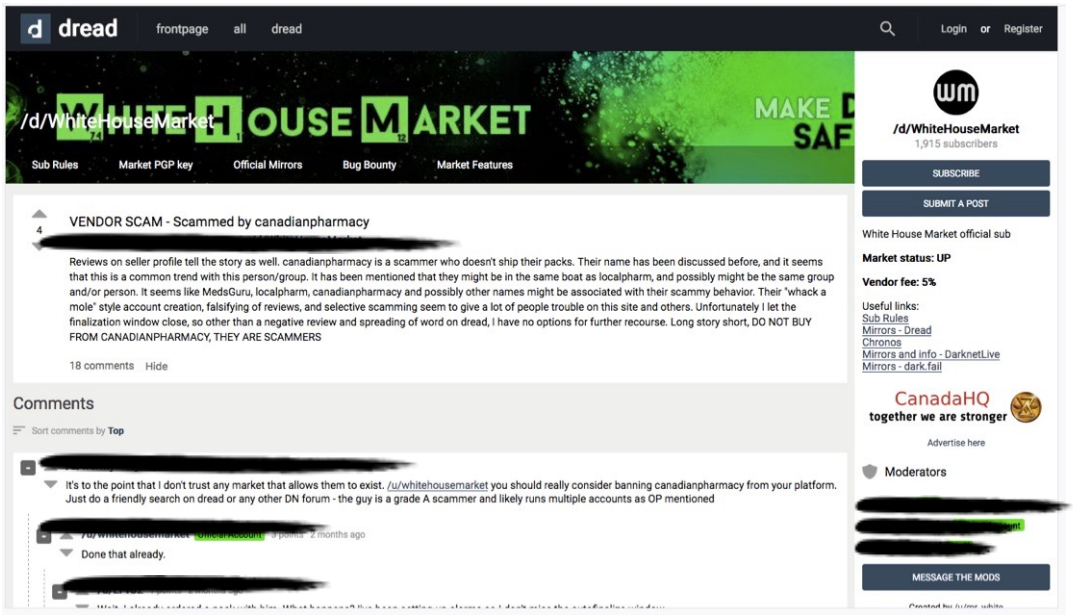


*Figure 5: Whitehouse Market forum posting on Vendor Scam*

Figure 6.0  depicts a user detailing their experience dealing with a particular vendor in order for other members to learn from their experience

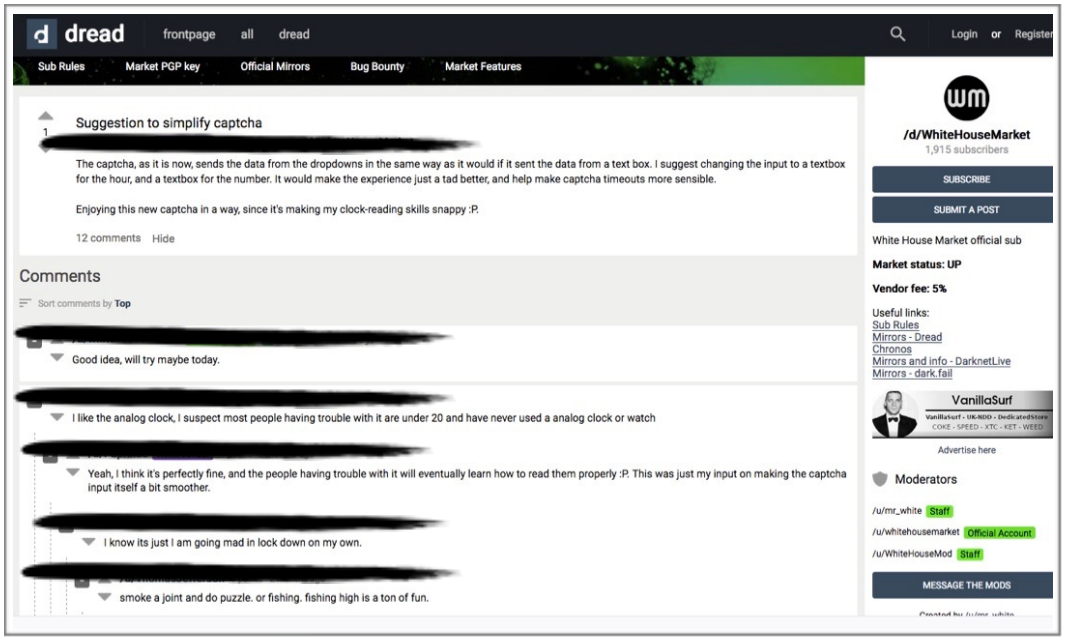


*Figure 6: Whitehouse Market forum posting on captcha suggestion*

Consequently, these communities offer an environment in which users can share ideas, practices, and recommendations about delinquent behaviour. Members of a community who share and reinforce one another's interests over time strengthen their delinquent bonds with one another. By increasing associations among delinquent peer groups involved primarily in deviant activities underground networks have the ability to influence reciprocal effects over time on social control and social learning. The reciprocal impacts of delinquent behaviour occur when users accept pro-delinquent norms and values through association with delinquent peers and common interest in purchasing illicit products. A significant amount of the emergence and development of community ties and engagements in the WHM can be attributed to user interactions. Through online interactions, users are able to form and maintain strong bonds through their mutual feelings, interests, and beliefs regarding illicit activities, which contributes to the longevity of these virtual communities within the dark web.

Unrestricted dissemination of information and opinions helps strengthen these relationships with the market. By sharing novel concepts, ideas, and opinions, both new and established members learn and adapt to the market. As a result of participating in discussion forums, users demonstrate a willingness to derive and reinforce delinquent values based on the quality, novelty, and relevance of the material discussed. Those attachments to pro-delinquent behaviour and norms are theoretically strengthened and reinforced when being associated with delinquent peers.

*Influences of Social Structure Characteristics*

In the context of social networks, common social value orientations, together with the concepts of social structure and community, can form the basis for understanding the network's main concepts, values, and goals. By participating in the market, users are able to set up social structures based on the similar goals, values, and behaviours of their members. It provides a social environment that can structure and influence behaviour, similar to the way common interests and values influence associations with members. Users who come together in an environment like the WHM can develop a reciprocal effect on peer group associations that are primarily involved in deviant behaviours. Peer-group associations' characteristics, accepted norms, and behaviours are strongly influenced by the structural covariates of the market, whose primary purpose is to facilitate the trade of illicit drugs.

The more users engage and contribute to the market through frequent posting, the more it affects the social structure of the market. Across the community findings, there is an underlying assumption that users in small markets are more prepared to switch platforms and engage with other users that will ensure the market survives against external threats from other illicit markets or law enforcement agencies. As a result of this assumption of a community that embraces altruistic and non-commercial values, the WHM elevates the relationship beyond efficient trading of products. In Figure 7.0, we see

members using the forums to reach out and provide assistance to others who are less experienced.

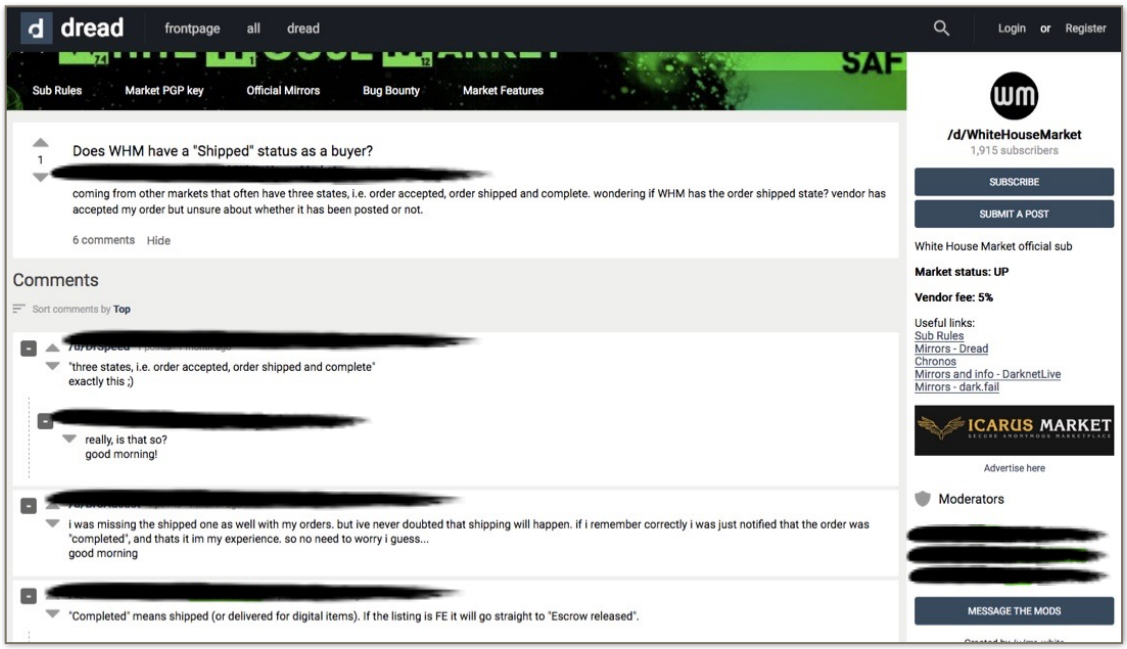


*Figure 7: Whitehouse Market forum post of member question*

*Shared values*

The relationship between users is founded upon their mutual interest in facilitating the trade of illicit drugs on cryptomarkets. According to this idea, different individuals enter the market in a variety of positions based on their interest in illicit operations. A constant posting of delinquent ideas, operations, and behaviours can also encourage members to engage in illicit activities. Posts made by members of the WHM do not reflect the opposite type of behaviour, reinforcing and influencing reciprocal social bonds on delinquent behaviour based on the similar values that each member shares and constantly reinforces and influences one another. Through open discussions found within the forum, shared values can be intensely increased as a result of product inquiries, reviews, and recommendations.

Various users, moderators, and vendors utilize community warnings as a way to protect these values and interests to makes it difficult to penetrate the underground network and destroy it. Some of the most prominent examples of these external threats are warnings regarding potential phishing, DDoS attacks, and interceptions of health packages. In addition, members will warn one another when there are issues with various vendors, such as scams. As a result of such protection measures, self-disclosing attitudes are maintained, which attracts social support within the market. An example of a DDoS attack warning on the market can be seen in Figure 8.0

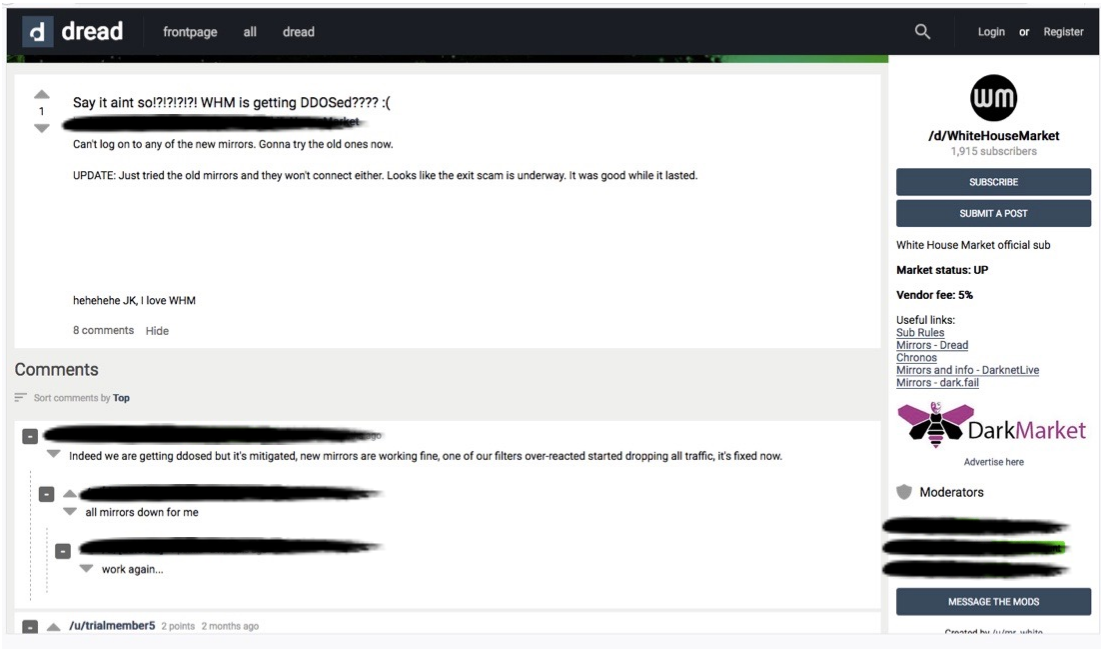


*Figure 8: Whitehouse Market forum post on DDosing*

The purpose of WHM is to increase the level of support that every member receives when protecting their activities and operations. Market support plays a crucial role in retaining members and possibly strengthening the safety of using these spaces for these illicit activities that also impact individual delinquent behaviours, bonds, and values. Communities consist of members who look out for one another based on the users' shared values. A key component of the WHM's informal institutional framework is

its feedback mechanism and vendor reputation, which provide enough confidence and momentum without government intervention.

Consumer demand is equally affected by communications on the market, which primarily manifest themselves in peer reviews and vendor marketing. Demand from consumers enables the community to become a valuable resource and creates amplification channels for members to share information, practices, and recommendations to strengthen community values and become a valuable resource for delinquent activities. The dimensions of shared values may eventually lead to reciprocal effects on delinquent behaviour, particularly through the associations of peer groups that can increase individuals' acceptance of delinquent norms and delinquent behaviour.

Limitations of the Findings

Due to the nature of this analysis, the interactional theory can only provide partial support for reciprocal effects on social learning and social control impacting delinquent behaviours within illicit marketplaces, tool-kits, and communities associated within the dark web. This limitation can be attributed to the fact that the forum emphasizes individual interactions through numerous comments and posts. Additionally, the interactional theory fails to identify whether pre-existing weakened attachments to conventional society or individual pre-attachments to pro-delinquent behaviour are impacted by the dark web. Moreover, the data fails to take into account if participation within the dark web leads to the dilution of attachments and bonds to normative society. Thus, the findings can not account for the full integration of Thornberry's (1987) interactional theory, as the individual engagements within the forum is limited to being able to explain or explore how the marketplace, illegal tool-kit, and community impact reciprocal effects on social learning and social control, while simultaneously impacting normative bonds to conventional society.

## Chapter 6: Discussion

The focus of this section will be to discuss how the interactional theory accounts for the dark web's marketplace, illegal toolkit, and community impacting and influencing delinquent behaviour, as well as the limitations of the interactional theory failing to account for wether or not it affects the weakening of conventional social bonds.

### Marketplace

*Provision of an Anonymous Environment*

The provision of the anonymous environment afforded to these dark web marketplaces has provided individuals with new ways to act and operate in underground networks. Through anonymized technology, the dark web has created more security and privacy levels that have influenced illegal activity and operations. As previously outlined, anonymous features like PGP keys, encrypted end-to-end messages, and crypto wallets are all used for confidential transactions and illicit operations. The interactional theory can account for the marketplace's provision of an anonymous environment creates spaces of safe havens to conduct a wide range of criminal activities. Described by Thornberry (1987), the interactional theory holds that crime and deviance are behavioural outcomes caused by environmental factors. The anonymous technology of the marketplace enhances the potential of creating environments that are free from conventional constraints, which may increase the possibility that individuals will engage in illicit behaviour. It is because of the opportunity for new freedoms and the inability to receive proper reciprocal feedback that an individual can channel his or her behaviours into delinquent committed patterns. Thornberry (1987) stated that environments that permit individuals to risk adjudication of minor or major delinquent actions can influence the outcome of delinquent behavioural attitudes. Through layered encryption, the anonymized markets of the dark web allow users to engage in delinquent behaviour since their identities are obscured and identification of their activities highly difficult to track (Du, 2020). Due to the weakening of conventional fears of incriminated by law

enforcement, a much broader array of behaviour can be permissible, becoming a powerful predictor of engagement in delinquent behaviour on the dark web.

Anonymized marketplace technology enables enhanced levels of encryption that create warrant-proof spaces that act as technological black boxes that relatively create impermeable environments to outside infiltration (Bellaby, 2018). Due to the lowering of prevention mechanisms by criminals to engage in crime and deviance, the interactional theory can account that the likelihood of crime and deviance being highlighted at the individual level can be influenced through the provision of anonymity environments and impact the social control of an individuals willingness to engage in criminal behaviour. Environments that create warrant-proof spaces, such as the dark web, can influence and affect the way individuals form relationships, model themselves, and reinforce their behaviours to more deviant. This association with illicit operations can lead to the development of increased delinquent values with a causal significance heightened by illicit operations (Thornberry, 1987). When this occurs, the interactional theory can explain that technological innovations like PGP and crypto can increase individuals' freedoms for the possibility to engage in any behavioural pattern they choose, resulting in these anonymous environments having a stronger influence on individual delinquent behaviours toward the participation of illicit activities.

The Whitehouse market demonstrates this to which encrypted tactics can influence delinquent behaviour through preventing user identities from being revealed, in turn improving social control over one's behavioural patterns and teaching individuals how to disguise their identity. Exposure to delinquent environments can directly influence delinquent behaviours that can ultimately determine a person's behaviour and social position (Thornberry, 1987). Individuals who have strong pre-existing bonds to illicit substances make these virtual markets more enticing due to the increased ease of distributing illicit products, and increasing its influence on individual delinquent behaviour and effect of reinforcement to consistency return to these markets. The social

control of these environments can strengthen bonds to delinquent behaviours when individuals become convinced that these environments are safe and allow them to act as they please (Thornberry, 1987). Thornberry (1987) would suggest that individuals who are free from conventional constraints and value these markets for the purpose of purchasing or selling illicit substances can create strong reciprocal relationships with delinquent values that can be sustained by the variables of anonymization technologies. Therefore, these anonymous environments can influence individuals values to deviance because they provide a space that can create new freedoms, opportunities, and interactions that encourage, develop, and perpetuate delinquent behaviour.

*Internet-Mediated Communication*

As, previously outlined in the findings, Internet-mediated communication typically involves exchanges of written, audio-visual, and multimodal messages with an oral connotation (Yus, 2011). The Internet advancements have transformed the concept of place – which traditionally referred solely to local communities – to incorporate non-local communities without physical or geological support (Lee, 2010). The advancements of the Internet have created new advancements in communication tactics within the dark web, where in particular the realization of end-to-end tunnel encrypted messaging has enabled a massive increase in private communication between users. The use of these new advancements of private communication, as outlined within the findings has increased interactions between users on these platforms that have impacted alongside both, the movement of illicit products and the development of deviant relationships.

Adapting the interactional theory can account for advancements in Internet-mediated communication within the dark web because they display influence on delinquent behaviour and provide a wide range of privacy and security controls that allow individuals to freely interact with others (Lee, 2010). As a result, they allow users to create and maintain relationships with delinquent peers, which may in turn influence

delinquent behaviour through the purchasing and selling of illicit products. As well, the interactional theory can explain how Internet-mediated communication advancements have also increased the association with delinquent peer groups that potentially can lead to the increase of the causal significance of delinquent values in the dark web (Thornberry, 1987). Delinquent peer group association increases along with increased access to information about the availability of drugs and products, which demonstrates that the interactional theory can explain that the strengthening of bonds and relationships with delinquent peer groups can be contributed by the increased communication and peer association that is afford by these advanced communication tactics.

Among the strongest predictors of deviance, Thornberry et al. (1994) argued that individual beliefs influence behaviour, albeit only weakly. In essence, when individuals are able to communicate easily and instantly, they are better able to form close associations with deviant peers. Consequently, the associations lead to an individual's sustained delinquent behaviour as they constantly influence and reinforce behaviours that increase the likelihood of sustained deviance. Through advanced encryption technology and tunnelled messaging, the international theory can take into account the fact that Internet-mediated communication may increase one's association with delinquent peers, thereby expanding the opportunity to engage in delinquent behaviour. By allowing delinquents to freely operate, they can reinforce delinquent values and behaviours, by being able to speak privately about illicit operations. As such, these spaces provide greater protection from external detection, which can influence an individual's behaviour by minimizing their potential for being caught.

The interactional theory can also recognize how Internet-mediated communication tactics have a significant impact on delinquent behaviour by allowing them to inspire behavioural and social change based on lower-risk advanced communication. A high level of privacy, a rapidly developing market, and the speed of communication available to users could theoretically change the way users bond, feel,

and behave within the marketplace. Individuals become associated with more delinquent peers as opportunities to commit delinquent acts increase, and they are thus more likely to become bonded to the delinquent peers that may increase the chances for them to engage in criminal and delinquent behaviour. With the advent of PGP and tunnelled encryption messages, it becomes easier to develop delinquent attitudes and behaviours, and associate with delinquent peers (Thornberry, 1987).

*Echo Chambers*

As previously, outlined echo chambers impact deviance wherein users are exposed to routinely reinforced delinquent norms and values. Echo chambers influence deviance by mirroring an individual's viewpoints and affirming them, while simultaneously enhancing the distortion of alternative perspectives (Wolleback, 2019). Among the factors responsible for echo chambers are confirmation bias, a process through which existing convictions reinforce the socially acceptable and desirable values of the environment (Wolleback, 2019). Its unique ability is to bring together like-minded individuals and perspectives that makes the online world a prominent platform for echo chambers to grow and develop (Wolleback, 2019).

The interactional theory can account for the development of echo chambers impacting delinquent behaviour within dark web marketplaces due to the fact that users of these spaces are mostly exposed to peers who share similar beliefs about the movement of illicit products within the marketplace. Previously, the findings of the Whitehouse market demonstrated that users engage in discussions where they echoed similar opinions about products, anonymity technology, and recommendations or questions pertaining to illicit trades. The constant repetition of similar values and opinions leads to a developing sense of identity that penetrates to an affect on an individual's behaviour through relationships with delinquent peers (Thornberry, 1987). Deviance is likely to precede one's involvement in delinquent behaviour, and exposure to

delinquent peer groups is both directly and indirectly responsible for such participation. This is especially the case when their collective delinquent values and opinions continue to be reinforced over time (Heimer & Matuesda, 1994).

It can be accounted for by the interactional theory that delinquent behaviour is constantly echoed within these spaces through the discussion and movement of illicit products. Thornberry (1987) explains that delinquent behaviours emerges through the association of others who influence and reinforce normative and behavioural models of deviance, and who motivate intrinsic and extrinsic reinforcement of delinquent behaviour to commit expressive behaviour. The relationship with peer groups makes these marketplaces ideal for the strengthening of individual bonds to deviance because they encourage normative behaviour (Thornberry, 1987). In the interactional theory, this can be attributed to the fact that users encourage delinquent behaviour in the marketplaces by distributing illicit substances and creating an environment in which specific delinquent activities are glorified at the expense of opposing lifestyles. Through their constant association with delinquent peer groups, delinquent behaviours and illicit operations are echoed throughout the market, which in turn results to the reinforcement of positive acceptance of delinquent values (Thornberry, 1991).

Markets create underground spaces that provide users with a high level of operational freedom without the repercussions associated with traditional delinquent behaviour. Based on the interactional theory (1987), marketplaces increase delinquent behaviours and norms by enhancing the privacy, protection, and security of users, while decreasing external controls like laws and the law enforcement agencies. A person's likelihood of engaging in deviance may be enhanced by the constant encouragement and association with delinquent peers who engage in criminal activities that can influence their own. According to Akers (1998), the emulation of deviant behaviour by delinquent peers is the best indicator of the onset, persistence, or avoidance of deviance. Deviant peers who constantly echo patterns of delinquent behaviour are indicators of delinquent

behaviour within themselves, and the influences of these deviant peers can become the determinant of a person's ultimate behaviour and social position over time (Thornberry, 1987).

## Illegal Tool-Kit

### *Technological Advancements*

Technological advancements within the dark web provide users with the ability to converse with one another and facilitate the distribution of illicit drugs. Utilizing technology on the dark web provides users with the ability to learn, perform, and reinforce delinquent behaviours (Thornberry, 1987). The anonymizing technology employed on the Whitehouse market creates this outlined 'privacy-plus' environment that creates protective barriers that made it near-impossible for outside intrusions (Bellaby, 2018). Taking into consideration technological advancements can impact delinquent behaviour, especially through learning new software and technology mechanisms that will open the possibility of committing various delinquent acts effortlessly on the dark web.

The evolution of encryption and technology that shields users' activities can manifest into the rise of delinquent behaviour in two ways. First, individuals are taught how to use these tools, which may be later utilized in committing illicit acts and subsequently reinforce the tendency of individuals to delinquent behaviours. Second, technological advancements such as PGP and encrypted messaging can appear as a catalyst for an increase in behaviour and attitude consistency within the conventional realm (Thornberry, 1991). According to the interactional theory, these tools can help reduce users' risks of being caught, while increasing their chances of obtaining rewards from participation in illicit activities. Due to mechanisms in place to protect user identities and operations, deviance in these underground spaces can be magnified, allowing for the constant influence of illicit behaviour.

Providing effective mechanisms for the purchase and sale of illicit products on the dark web, these tool-kits give users more opportunities to learn and engage in delinquent behaviour. Technological tools play a critical role in helping shape a social context that directly affects the bonds formed between users and illicit marketplaces during the transaction of illicit goods (Thornberry, 1987). By leveraging anonymization technology, the dark web becomes a space where individuals can be incentivized by the ability to distribute illegal goods privately. It accounts for the impact of technology on deviance that involves reciprocal effects on social control and social learning since the tools are able to teach individuals how to operate in these illicit markets as well as influence social factors that affect their behaviour over time (Thornberry, 1987). In this way, the interactional theory can accounts for an important variable that can predict and determine an individual's future delinquent behaviour. As a consequence, individuals using these technological applications are most likely to engage in delinquent market behaviour. Therefore, it seems that these technological tools and the latent dimensions of illicit deviance have a causal connection (Thornberry, 1987).

*Learning from Peer Association*

As, previously outlined within the findings, the interactional theory can also explain how users learn delinquent values from associations with delinquent peer groups. According to Thornberry (1987), delinquent behaviours are influenced by learning environments, especially those that channel behavioural freedoms into delinquent behaviour. Dark web associations with delinquent peers provide a learning environment where individuals can engage in effective interactions and collaborative learning from delinquent peers. The ability to reinforce these values and behaviours through associations and engagements with delinquent peers can also influence behavioural and attitudinal consistency (Thornberry, 1987). The ability to exhibit delinquent behaviour in social interactions and form stronger relationships with delinquent peer groups may be responsible for increased attachment to deviance. Due to these relationships, associations

with delinquent peers on the dark web may account for developmental changes and the significance of delinquent values that become more fully articulated with illicit operations that can be influenced by delinquent behaviour (Thornberry, 1987).

Delinquent behaviours can also be influenced through associations with other members (specifically, delinquent peers) that allow individuals to learn and reinforce these delinquent values and behaviours (Thornberry, 1987). These developmental processes are stimulated when individuals pose a mixture of questions concerning delinquent operations to experienced users. As a result of these interactions, users tend to engage in delinquent behaviour by asking "how-to" questions or seeking advice regarding the proper use of encrypted features to conceal the purchasing of illicit products. As illustrated in the outlined forum posts, users are motivated to engage in market activities and sustain their engagement throughout the interactional process (Thornberry, 1987). As described here, the interactional theory proposes that the association between individuals and peer groups acts like a technical tool-box that influences their engagement in criminal behaviour by inspiring them to learn and perform illegal activities. Individuals who have difficulty learning to utilize these spaces may pull themselves away from the environment, reducing their bonds to deviance. However, if they are able to exploit these associations, it may play a role in them learning how to operate in these spaces, and have a direct impact on their engagement with illicit operations in the future. Overall, the interactional theory can account that associations with delinquent peer groups can impact delinquent values and create strong reciprocal relationships with delinquent behaviour (Thornberry, 1987).

## Community

### *Common Interests Strengthening Bonds*

The dark web is a form of community where various individuals come together over shared interests. As defined by Owens (1998), an online community is a group of individuals who regularly interact and share common goals, ideas, and values. Those with a similar enthusiasm for pro-delinquent behaviour can be inspired by the anonymity and advanced encryption provided by the dark web. The findings from the study suggest that spaces on the dark web can strengthen social bonds and contribute to delinquent behaviour by shaping attitudes and ideas that can potentially transform into individual behaviour. It helps strengthen mutual interests when users share ideas about how to improve various aspects of security, speed of communication, or create additional purchasing methods. The interactional theory posits that underground environments act as a network which strengthens social ties by exchanging information, sharing experiences, and reaffirming rules and values that define individuals (Lee, 2010). Members of these communities share common interests, providing a sense of belonging they do not feel they can find in conventional society.

Using the interactional theory, it can be argued that anonymized platforms enable more intimate and open discussions, thereby encouraging users to discuss criminal activity. The associations and interactions between users allow individuals to advance criminal behaviour by being able speak openly and seek the information that they need, without the need to be cautious. According to Thornberry (1991), three items best embody delinquent-oriented dimensions that influence delinquent behaviour. The interactional theory can account that the dark web networks reinforce and enforce group interests (1), they increase engagement in pro-delinquent activities or discussions (2), and advance the commitment to delinquent behaviours (3). By bringing together those who are common interests revolving pro-delinquent behaviour, can reinforce pro-delinquent norms through constant interactions.

*Social Structure Characteristics*

Another hypothesis of the interactional theory explaining how the underground network influences delinquent behaviour is through the idea that behaviour follows a trajectory sparked by the environment's social structure (Thornberry, 1987). A dark web community is built upon the structure of social roles and statuette of the individuals who make up the community. A community's social structure helps in conceptualizing the side-by-side differentiation of its desired goals and values. As a result of the structural characteristics of these online communities, behaviour norms and values are transmitted and influenced (DeSanctis & Poole, 1994). As a result, online community members will be more likely to connect with each other because they believe they are generally helpful, trustworthy, and somewhat useful (Patulny, 2005). As previously mentioned, members of the forum trust one another's advice on topics such as escrow, illicit products, and vendors. As a result, it appears that online users have a cooperative relationship with one another and provide each other with communication, information, and emotional support (Lee, 2010).

As discussed previously, the WHM members share similar goals, interests, and values pertaining they movement and distribution of illegal goods. Through member interactions, familiar social environments are formed that directly influence each individual. As a consequence of these market structures, delinquent values are influenced and reinforced, laying the foundation for individuals to associate with peer groups that are primarily engaged in delinquent activities. In this group, there's a higher likelihood of repeating criminal behaviour because of the social structure that influences the communities activities. Thornberry and Krohn (2005) argue that social structures that promote delinquent social bonds are causally responsible for advancing the impact on deviance within the community and likely to heighten these behaviours throughout. When individuals participate in environments like the dark web, its structure increases

protection and can increase deviant peer influence, which contributes to reciprocal effects on delinquent behaviour.

Overall, the interactional theory can account for the dark web's communities social structure to impact delinquent values and behaviours. It can either be a result of users' extensive engagement on the forum, or experienced members' willingness to provide assistance to those who are not as familiar with the community. Individuals' attachment to the community could be influenced by the effects of these structures, and delinquent behaviour could be affected by it as well (Thornberry, 1987). In turn, the structures enable users to associate with other individuals, thereby fostering peer association among user's. The characteristics of a pro-delinquent community can therefore lead to users acceptance of pro-delinquent norms, since active participation in distributing illicit products can also be seen as a predictor of continued involvement in delinquent behaviour.

*Shared Values*

It is possible to influence the relationships between delinquent values and the moral character of an individual through associations that share similar values of delinquent activities (Thornberry, 1987). As previously outlined, various threads within the WHM forum refer to new entrants to the market either as buyers or sellers, encouraging open discussion and connections. The interactional theory can account that distinct delinquent groups that share common values create distinctive trajectories of deviance with all individuals who are apart of the community (Thornberry, 1987). It can be argued that shared values within a community are responsible for increased measures of deviant peer association, as well as having a direct effect on bringing together those with a similar way of thinking. Deviant peer association plays an important role in the development of new social relations through the reciprocal relationship between social learning and social bonds (Thornberry, 1997). The encouragement of the community

promotes this development process, allowing members to interact with other pro-delinquents with similar values.

Communities built through common delinquent values have an impact on human behaviour and trajectory of criminal activity when viewed in the framework of interactional theory. Communities which are founded on shared values can create extensive relationships and new associations with peers that can reinforce and continue to strengthen the values of the community. Delinquent beliefs and values can continue to impact the overall community's behaviour, based on the conventional beliefs that tend to be shared among the community's users, which can lead to an increase of deviance. Individuals who share a common value within the dark web can increase peer group influences through increasing associations with those with similar interests. As a result of the constant association and communication with users, new concepts, ideas, and opinions are developed - increasing relationships and values of delinquent behaviour. As the dark web develops and forms communities of common values, delinquent values become more likely to become strong effects of criminal operations performed on the dark web.

Overall, interactional dynamics help explain how communities also impact delinquent behaviours through the attachments and relationships of individuals through their shared values of deviance that influence and regularly reinforce their illicit activities. The social interaction of the community can explain that it processes deviance and increases the likelihood of association with delinquent peers and delinquent behaviour through their formed relationships of shared values of delinquent behaviours (Thornberry, 1987). As a result, it creates a familiar social environment where bonds are directly influenced by one's values, beliefs, and norms. It indicates that those who share common values influence members' actions and normative beliefs within the community. Thus, the interactional theory would account that share values can directly lead to an increase of association with delinquent peers that reinforce and strengthen attachments to

pro-delinquent behaviours. The sharing of values in the dark web communities creates a social setting in which delinquent behaviours are learned, reinforced and effect patterns of deviance, delinquent peer group association, and acceptance of pro-delinquent norms.

### Limitations of the Interactional Theory

Thornberry (1987) emphasized through his work on the interactional theory that individuals develop weakening of conventional social bonds from the exposure of delinquent environments. Thornberry (1987) suggested that delinquent behaviour is a byproduct of social interactions, and should consequently be studied through interactive processes. In an amplifying loop, the elements of social control and social learning promote engagement in delinquent behaviours (Thornberry, 1987), as low social control increases the likelihood of an individual associating with delinquent peers. In turn, this strengthened social connection to pro-delinquent norms further weakens individual's attachments to normative values to conventional society. However, the interactional theory does not adequately address whether or not the dark web weakens social bonds towards conventional society either because users come into the dark web with pre-existing weaken bonds or because normative bonds are not diluted through the participation within the dark web.

### Social Bonds

Thornberry (1987) posits that in order for individuals to engage in deviance they must already have weakened attachments and bonds to conventional society. Having weak attachments to school or work, or weak relationships with parents, can prompt an individual to enter a delinquent environment to learn, perform, and reinforce delinquent behaviours (Thornberry, 1987). In his research, Thornberry (1987) outlines the possibility that delinquent behaviour may result from prior antisocial or delinquent behaviours. In the dark web, the interactional theory has trouble or fails to account for any pre-existing weakened social bonds to conventional society being present when individuals enter and engage within the dark web.

It is possible that users of the WHM may have had some prior connection to deviance outside the dark web, and start to engage in the market that primarily is used to for the movement of illicit substances. The argument can therefore be made that many of these users would have redirected their delinquent behaviour to the virtual realm and continued their illicit operations within these underground networks. Furthermore, the dark web may have been a transitional path for individuals who previously engaged in delinquent behaviour, especially offline vendors selling illicit substances on street corners. At the same time, buyers who traditionally purchased their products offline may have moved over to these virtual marketplaces in order to protect their identity and transactions with the use of layered encryption and the use of cryptocurrencies (Barratt & Aldridge, 2016). Although these possibilities can certainly be explored, overall the interactional theory is not able to account for whether or not individuals already have weakened bonds to conventional society. Individuals' use of the dark web may not be impacted and influenced by their previous delinquent behaviours and their formation of pre-existing pro-delinquent bonds. The dark web's impact on delinquent behaviour may also not need or require as Thonberry (1987) stated to have pre-existing weakened attachments and bonds to convention society in order to be vulnerable enough to join the delinquent environment. Furthermore, this means through the use of the WHM data, the interactional theory can not take into account whether or not individuals who join the dark web's underground environment needs or has present weakened attachments or antisocial behaviours prior to entering the dark web.

Dilution of Normative Bonds

The analysis on the interactional theory on the dark web also fails to account for whether or not Thornberry's (1987) proposed belief that as an individual develops and increases bonds with delinquent behaviours, it also further diminishes their social bonds to conventional society. As with prior studies by Elliott and Menard (1996) and Warr and Stafford (1991) on the interactional theory, the dark web is unable to explain this impact of users' attachments to normative society being affected as their behaviours and

attachments to delinquent values are strengthened through the participation of illicit activities within the dark web.

The evidence suggests that normative bonds and attachments on the dark web are either non-existent or cannot be accounted for from the evidence of the WHM that normative attachments are affected. It is possible that members are able to live a double life and maintain their conformity to society while engaging in delinquent acts on the dark web. As an alternative, it may not be required for an individual to decrease their normative attachments when participating in illicit underground markets and operations, as users may be able to comprehensively detach themselves from illicit environments. In his analysis of the dark web, Paul Dwyer (2020) points out that the dark web has "normalized the abhorrent" and allows individuals to detach themselves from its environment, as it is built with the security technology that allows users to mask their identities, allowing them to hide their normative lives online. Raab (2017) further notes that privacy is a constitutive public good, a component of society at large. By ensuring privacy, individuals are able to take advantage of opportunities on the dark web without sacrificing their normative lives and freedoms because of the technological advancements allowing them to not only mask their identities but create layers of encryption to separate themselves from their illicit operations.

A further argument could be made that the interactional theory cannot explain for the decreasing normative bonds on the dark web because unlike traditional causes, the dark web may not account for individuals' social structural characteristics (e.g. income, social class, and social status) affecting their delinquent trajectories. In contrast, these elements may not be present on the dark web, causing individuals to maintain their normative bonds to society, attachments, and values. Individuals may be engaging in illicit activities online purely to satisfy their urge to procure illicit substances, while not remaining fully invested in the delinquent lifestyle. Thus, the interactional theory may not be able to explain whether or not there are diminished normative bonds on the dark web.

Accordingly, Thornberry's (1987) traditional explanation on deviance may not translate on to the dark web, as it presents different variables than those affecting classical deviant behaviours.

Anonymous online personas allow individuals to maintain a separate identity offline while adopting other certain online personas (Chertoff & Simon, 2015). According to the research, there are no reports indicating that the WHM users' have weakened normative bonds. This indicates that users could remain active at home without compromising their normative lives through the use of anonymized technology and layered, tunnelled encryption on the dark web. In addition, it could also mean that traditional delinquent behaviour is usually easier to spot than they are on the underground network, and can be more challenging to spot and observe. In this sense, it is plausible that the dark web creates a series of networks where individuals can freely operate, conceal their identity, and maintain normal relationships and lifestyles. Overall, the dilutions of normative social bonds to conventional society fails to account for whether or not individuals within the dark web, especially illicit marketplaces, have any impact on the dilutions of normative social bonds to conventional society.

## Chapter 7: Conclusion

Thornberry (1987) argued that delinquent behaviour emerges in an interactive setting as a result of reciprocal effects on social learning and social control. The combination can lead to individual delinquent behaviour and delinquent bonds while simultaneously weakening normative bonds and values in conventional society. Recently, the dark web has been used extensively for distributions of illicit substances and other illicit operations. Although this powerful platform has increased its influence and impact on delinquent behaviour (Holt 2017), little theoretical attention has been given to it.

This study sought out to integrate the dark web research by conducting more of a theoretical approach by incorporating the interactional theory as a theoretical framework to describe the dark web as a marketplace, illegal tool-kit, and online community, and how those factors influence delinquent behaviour. The interactional theory was chosen because it is considered a model that combines both outcomes and predictors of deviance, presenting an ideal framework for identifying new associations (Hoffman, Erickson, & Spence, 2013).

As a result of the exploration analysis, the interactional theory was partially able to explain how the dark web manifested as a marketplace, illegal toolkit, and virtual community impacting reciprocal effects on social control and social learning on individual delinquent behaviours. Although the interactional theory could explain how delinquent behaviour is effected, influenced, and reinforced within the dark web, it was not able to or failed to account for the effects of weakening normative bonds. The collected data from the Whitehouse market either could not be utilized or could not account for whether user engagements on the dark web potentially affects the dilution or pre-existing attachments and bonds to normative society.

The study displays similar interactions where behaviours were structured and influenced by one another. Sociability and generalized norm predictors significantly influence online community structure (Lee, 2010). The study suggested that members share similarities in goals, behaviours, and values to commit buying and selling illicit products. The study found that user interactions form a familiar social environment where each member directly influences the other, as common interests were purchasing illicit products based on their value, price, quality, and shipping method. The findings suggested behaviour of members influences the structure of the market, leading to an interactively self-reinforcing constellation of delinquent communication (Thornberry, 1991). The market's structural covariates seemed to strongly influence peer-group associations' characteristics, accepting norms and behaviours based on the market's primary purpose of facilitating the trade of illicit drugs.

Due to its ephemerality, the illicit market was made possible by ephemeral technology, products, and structures. Peer-group affiliation, normative standards, and delinquent behaviours influence structural correlations as covariates of social values. In an interactive setting where illicit activity can be encouraged, delinquent behaviour can be influenced by association with others who share similar interests. (Thornberry, 1987) According to the evidence gathered, these interactive settings consistently shaped shared interests and values for promoting delinquent behaviours (Thornberry, 1997). Based on this reciprocal effect pattern, we can see that the dimensions of an environment that encourage peer group associations and acceptance of delinquent norms through the distribution of illicit products are embedded in a communication system that reinforces delinquent orientations and behaviours. In a social environment with opportunities for interactive learning, individuals can learn normative attitudes and lessen their animosity toward illegal activities. In turn, a normative orientation where individuals are traditionally drug users or dealers positively impacts the association and encourages these standards and behaviours.

The prevalence of peer groups and technological advances, as well as the desire to buy or sell illegal drugs, all contributed to the acceptance of pro-delinquent norms within the WHM. A low level of social control, according to the interactional theory, increases the possibility of participating in delinquent behaviours and involvement in deviant peer group relationships, which further reduces normative attachments (Thornberry, 1987). The results of this study displayed that the dark web can act as a market for people who traditionally distribute illegal drugs by either selling or buying them. It provides traditional drug dealers and users a place to anonymously distribute illegal substances, while staying hidden through techniques including encryption and the use of cryptocurrencies (Belaby, 2018).

As stated by Thornberry (1987), the interactional theory proposes that an individual's position in society is the initial factor contributing to deviant behaviour. The analysis displayed that control dynamics can systematically affect and influence deviant behaviour trajectories. On the basis of the dynamics presented, this can be interpreted as a developmental change in social controls that lead to the use of the dark web for illicit purposes. Technological advancements that make it easy to communicate, form relationships, and share illicit substances can influence social controls preceding individual delinquent behaviour. As a result, it creates opportunities for people to work and learn together based on their common interests and values, while ensuring their needs, wants, and activities are protected (Lee, 2010).

## Contributions and Implications of the Study

The major contribution throughout this explorational study was the development of a new theoretical framework of the interactional theory and how be integrated to account for the dark web as a marketplace, illegal tool-kit, and online community impacting individual delinquent behaviour. The study displayed that social interactions and interactive settings can play a crucial role in the emergence of deviant behaviour. As

well, it was able to portray the dark web as a set of technical characteristics, advanced networking system, and private ecosystems that can facilitate criminal activity. In addition, it revealed that the reciprocal effects on social control and social learning can explain delinquent behaviour and pro-delinquent bonds through the increase of associations with delinquent peer groups and advanced social interactions within the dark web (Thornberry 1987). The interactional model in this study proved to be an effective method to examine how the dark web can impact and influence individual delinquent behaviour while also appealing to broad audiences with similar values.

With the use of the interactional theory to explore other underground networks, the theoretical analysis can serve as a starting point for future research on the dark web. Research can be conducted in the future to investigate other interactions between delinquent peer groups, normative orientations, and behaviours that increase the risk of deviance in underground environments. Using Thornberry's (1987) interactional theory, there is potential for this study to be extended to explore and analyze other aspects, questions, and elements of the dark web.

Overall, this dissertation's contribution is its creative and innovative use of the interactional theory to analyze the dark web's characteristics as a marketplace, illegal tool-kit, and online community impacting users' social bonds, values, and likelihood of engaging in delinquent behaviour. This research contributes (1) to understanding the dynamics impacting self-reinforcing reciprocal effects within an interactive social setting. (2) Understanding how reciprocal relations on social learning and social control variables impact deviance. (3) The role of technology, innovation, and community structure further facilitating exposure to delinquent behaviours. (4) The advancing communication and heightened social controls of peer group associations influencing the meaning of community and creating network structures to share similar values and interests.

As of today, research on the dark web has lacked many theoretical contributions in terms of examining delinquent causations. Studies have often ignored to explore whether or not interactive settings increase likelihood of associations with delinquent peer groups and the adoption of delinquent behaviours (Thornberry, 1987). An empirical study suggests that interrelationships between markets, tool-kits, and communities can be viewed as self-reinforcing cycles of deviance. A pre-existing need for the distribution of illicit substances, technologies such as PGP, and the ability of members to interact and create opportunities to reinforce delinquent behaviour. Furthermore, these findings underscore the significance of the theoretical expansion on research that can better understand virtual spaces and their impact on delinquent behaviour (Bossler & Holt, 2014). This research is among the first to look at the interactions between the accusation of delinquent peers, adaptation to pro-delinquent norms, and criminal behaviour in the context of proximate dynamics of illicit causation in the dark web using a longitudinal approach. It also lays the groundwork for focusing on the influence of social structural factors, technological advancements, and traditional value orientations on delinquent behaviour via dark web environments.

Ultimately, the studies implications indicates that the theoretical framework provided a useful way of understanding and addressing the dark web as a cause of individual deviance, and as an important stepping stone for future theoretical explorations on the dark web. The issue remains that while the interactional theory may account for the dark webs impact on deviance especially as it pertains to the platform's manifestation as a marketplace, illegal tool-kit, and community, it fails to account whether or not deviance impacts social normative bonds to conventional society. In light of this, future research should address the theoretical framework of deviance in the dark web in two ways. It could look to examine whether or not the interactional theory could be extended to other forums on the dark web, such as terrorism, right-wing extremism, or political corruption based on the fact that this analysis focused primarily on an illicit drug market. The second, further research agendas could look to use another theoretical framework

that could potentially account for pre-existing weakened or the dilution of normative bonds to society, or possibly develop a new theoretical framework that could account for these variables of weakened social bonds within the dark web.

## References


Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behaviour in the age of information. Science (New York, N.Y.). 347. 509-14. 10.1126/scence.aaa1465.

Afilipoaie, A. and Shortis, P. 2015. *From Dealer to Doorstep–How Drugs are Sold on the Dark Net.* Global Drug Policy Observatory, Situation Analysis.

Albers, M. J. (2017). Quantitative Data Analysis—In the Graduate Curriculum. *Journal of Technical Writing and Communication*, *47*(2), 215–233. https://doi.org/10.1177/0047281617692067

Aldridge, J., & Decary-He´tu, D. (2014). Not an 'Ebay for Drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. Available at SSRN 2436643.

Al Nabki, W., Fidalgo, E., & Alegre, E. & Paz, Ivan. (2017). Classifying Illegal Activities on Tor Network Based on Web Textual Contents. 35-43. 10.18653/v1/E17-1004.

Akers, R. L. 1998. Social Learning and Social Structure: A General Theory of Crime and Delinquency. Boston: Northeastern University

Asatani, K., Toriumi, F., Ohashi, H. (2014). Rise and decline process of online communities: Modelling social balance of participants. In: Miguel, F. J., Amblard, F., Barceló, J. A., Madella, M. (Eds.), Advances in computational social science and social simulation (pp. 329–338). Universitat Autònoma de Barcelona.

Bartlett, J. 2014. Dark Net Markets: The eBay of Drug Dealing. *The Guardian*, 5 October. http://www.theguardian.com/society/2014/oct/05/dark-net-markets-drugs-dealing-ebay.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets (but were afraid to ask). *The International Journal of Drug Policy*, *35*, 1–6. https://doi.org/10.1016/j.drugpo.2016.07.005

Barratt, Monica J., and Alexia Maddox. "Active Engagement with Stigmatised Communities through Digital Ethnography." Qualitative Research, May 22, 2016, 1468794116648766. doi:10.1177/1468794116648766.

Baerveldt C, Völker B and Rossem R van (2008) Revisiting selection and influence: An inquiryinto the friendship networks of high school students and their association with delinquency. Canadian Journal of Criminology and Criminal Justice, 50:559–587.

Bellaby, R. (2018). Going dark: anonymising technology in cyberspace. *Ethics and Information Technology*, *20*(3), 189–204. https://doi.org/10.1007/s10676-018-9458-4

Bernstein, A., Marshall, E., & Zvolensky, M. (2011). Multi-Method Evaluation of Distress Tolerance Measures and Construct(s): Concurrent Relations to Mood and Anxiety Psychopathology and Quality of Life. *Journal of Experimental Psychopathology*, *2*(3), 386–399. https://doi.org/10.5127/jep.006610

Beshiri, A.S. and Susuri, A. (2019) Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. Journal of Computer and Communications, 7, 30-43. https://doi.org/10.4236/jcc.2019.73004

Biryukov, A., Pustogarov, I., Thill, F. and Weinmann, R.P. 2014. Content and Popularity Analysis of Tor Hidden Services. In *Distributed Computing Systems Workshops (ICDCSW), IEEE 34th International Conference*; 30 June–3 July, Madrid, Spain: IEEE.

Boers K, Seddig D and Reinecke, J (2009) Sozialstrukturelle Bedingungen und Delinquenz im Verlauf des Jugendalters: Analysen mit einem kombinierten Markov-undWachstumsmodell. Monatsschrift für Kriminologie und Strafrechtsreform, 92(2/3): 267–288.

Boyd, danah m, & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Bradbury, D. (2014). Unveiling the dark web. *Network Security*, *2014*(4), 14–17. https://doi.org/10.1016/S1353-4858(14)70042-X

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An
analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology, 8(1), 1-20. Retrieved from http://search.proquest.com.uproxy.library.dc-uoit.ca/docview/1545341663?accountid=14694

Brugnoli, E., Cinelli, M., Quattrociocchi, W., & Scala, A. (2019). Recursive patterns in online echo chambers. *Scientific Reports*, *9*(1), 20118–18. https://doi.org/10.1038/s41598-019-56191-7

**Buxton, J. and Bingham, T. 2015. *The Rise and Challenge of Dark Net Drug Markets*. Global Drug Policy Observatory. Policy Brief No. 7.**

**Byrne, J.M., and K.A. Kimball. 2017. Inside the Darknet: Techno-Crime and Criminal Opportunity. In *Criminal Justice Technology in the 21st Century*, 3rd ed, ed. L.J. Moriarty, 206–232. Illinois: Charles C. Thomas Publisher.**

**Catalano, R. F., & Hawkins, J. D. (1996). The Social Development Model: A Theory of Antisocial Behavior. In J. D. Hawkins (Ed.), Delinquency and Crime: Current Theories (pp. 149-197). New York: Cambridge University Press.**

*Chertoff, M.(2017) A public policy perspective of the Dark Web, Journal of Cyber Policy, 2:1, 26-38, DOI: 10.1080/23738871.2017.1298643*

Chertoff, M. and Simon, T. 2015. *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance. Paper Series No. 6.

Childs, K., Sullivan, C., & Gulledge, L. (2010). Delinquent Behavior Across Adolescence: Investigating the Shifting Salience of Key Criminological Predictors. Deviant Behavior, 32(1), 64–100. https://doi.org/10.1080/01639621003748498

Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deepweb and Cybercrime. Trend micro report. Retrieved from https://www.trendmicro.de/cloudcontent/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC Medical Research Methodology, 11(1), 100–100. https://doi.org/10.1186/1471-2288-11-100

Cromwell, P. F., & Olson, J. N. (2004). Breaking and entering: Burglars on burglary. Thomson/Wadsworth.

*Darren R. Hayes, Francesco Cappa, & James Cardon. (2018). A Framework for More Effective Dark Web Marketplace Investigations. Information, 9(8). https://doi.org/10.3390/info9080186*

*Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. Global Crime, 13(3), 160–175. https://doi.org/10.1080/17440572.2012.702523*

*DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. Organization Science (Providence, R.I.), 5(2), 121–147. https://doi.org/10.1287/orsc.5.2.121*

Dingledine, Roger & Mathewson, Nick & Syverson, Paul. (2004). Tor: The Second-Generation Onion Router. Paul Syverson. 13.

*Dolliver, D.S. 2015. Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel. International Journal of Drug Policy 26 (11): 1113–1123.*

*Du, K. (2020). A Market in Dream: the Rapid Development of Anonymous Cybercrime. Mobile Networks and Applications, 25(1), 259–270. https://doi.org/10.1007/s11036-019-01440-2*

Dumbach M. (2014) Theoretical implications. In: Establishing Corporate Innovation Communities. Markt- und Unternehmensentwicklung / Markets and Organisations. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-03695-9_24

Ebneyamini, S., & Sadeghi Moghadam, M. (2018). Toward Developing a Framework for Conducting Case Study Research. International Journal of Qualitative Methods, 17(1), 160940691881795–. https://doi.org/10.1177/1609406918817954

**Elliott, D. S. 1985. "The Assumption That Theories Can Be Combined with Increased Explanatory Power:Theoretical Integrations." In Meier R. F. (Eds.), Theoretical Methods in Criminology. 123-149. Beverly Hills, CA: Sage.**

Elliott, D. S., S. S. Ageton, D. H. Huizinga, B. A. Knowles, and R. J. Canter. 1983 The Prevalence and Incidence of Delinquent Behavior: 1976-1980 (National Youth Survey Report No. 26). Boulder CO : Behavioral Research Institute.

Elliott, D. S., and S. Menard. 1996. "Delinquent Friends and Delinquent Behavior: Temporal and Developmental Patterns." In Hawkins D., (Eds.),Delinquency and Crime: Current Theories 28 - 67. New York, NY: Cambridge University Press.

Finklea, K., & Theaohary. C. (2015). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. Congressional Research Service. https://ipmall.law.unh.edu/sites/default/files/hosted_resources/crs/R42547_120720.pdf

Flyvbjerg, B. (2011). Case study. In Denzin, N. K., Lincoln, Y. S. (Eds.), The Sage handbook of qualitative research (pp. 301–316). Thousand Oaks, CA: Sage.

Garg, V., & Camp, L. J. (2015). Why cybercrime? ACM SIGCAS Computers and Society, 45(2), 20-28. doi:10.1145/2809957.2809962

*Gehl, R. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. New Media & Society, 18(7), 1219–1235.*

Goodison, Sean & Vermeer, Michael & Barnum, Jeremy & Woods, Dulani & Jackson, Brian. (2019). Law Enforcement Efforts to Fight the Opioid Crisis: Convening Police Leaders, Multidisciplinary Partners, and Researchers to Identify Promising Practices and to Inform a Research Agenda. 10.7249/RR3064.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405

Hellström I, Nolan M, Lundh U (2005).'We do things together': A case study of 'couplehood' in dementia. Dementia. 2005, 4: 7-22. 10.1177/1471301205049188.

Heimer, K., & Matsueda, R. L. (1994). Role-Taking, Role Commitment, and Delinquency: A Theory of Differential Social Control. *American Sociological Review*, *59*(3), 365–390. https://doi.org/10.2307/2095939

Hirschi, T.(1969). Causes of Delinquency, Berkeley: University of California Press

*Holt, T. (2017). Identifying gaps in the research literature on illicit markets on-line. Global Crime: Illegal Markets in Cyberspace, 18(1), 1–10. https://doi.org/ 10.1080/17440572.2016.1235821*

*Holt, T. (2013). Exploring the social organisation and structure of stolen data markets. Global Crime., 14(2), 1–20. https://doi.org/info:doi/*

*Holt, T. (2013). Examining the Forces Shaping Cybercrime Markets Online. Social Science Computer Review, 31(2), 165–177. https://doi.org/10.1177/0894439312452998*

*Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. Deviant Behavior, 35(1), 20-40. doi:10.1080/01639625.2013.822209*

Holt, T.J., & Lampke. E. (2010), "Exploring stolen data markets online: products and market forces," Criminal Justice Studies, vol. 23, no. 1, pp. 33–50, 2010. [Online]. Available: https: //doi.org/10.1080/14786011003634415

HOFFMANN, J., ERICKSON, L., & SPENCE, K. (2013). MODELING THE ASSOCIATION BETWEEN ACADEMIC ACHIEVEMENT AND DELINQUENCY: AN APPLICATION OF INTERACTIONAL THEORY. *Criminology (Beverly Hills)*, *51*(3), 629–660. https://doi.org/10.1111/1745-9125.12014

Horton-Eddison, M., and M. Di Cristofaro. 2017. Hard Interventions and Innovation in Crypto-Drug Markets: The Escrow Example, 11. Policy Brief: Global Drub Policy Observatory.

Hughes, D., Rodriguez, J., Smith, E., Johnson, D., Stevenson, H., & Spicer, P. (2006). Parents' Ethnic-Racial Socialization Practices: A Review of Research and Directions for Future Study. *Developmental Psychology*, *42*(5), 747–770. https://doi.org/ 10.1037/0012-1649.42.5.747

Iliou, C., Kalpakis, G., Tsikrika, T., Vrochidis, S., & Kompatsiaris, I. (2017). Hybrid focused crawling on the Surface and the Dark Web. *EURASIP Journal on Information Security*, *2017*(1), 1–13. https://doi.org/10.1186/s13635-017-0064-5

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. New Media & Society, 20(2), 435–452. https://doi.org/10.1177/1461444816639976

Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Global Commission on Internet Governance. Paper Series No. 21.

Junghee Lee, & Hyunjoo Lee. (2010). The computer-mediated communication network: exploring the linkage between the online community and social capital. *New Media & Society*, *12*(5), 711–727. https://doi.org/10.1177/1461444809343568

Krebs, B. (2017). "Tax Fraud Advice, Straight From the Scammers," Krebs on Security, March 24, 2015.

Kirkpatrick, K. (2017). Financing the Dark Web. Communications of the Association for Computing Machinery, 60(3), 21–22. https://doi.org/info:doi/

*Kinklea, K. (2017). Dark Web. Congressional Research Service. https://fas.org/sgp/crs/misc/R44101.pdf*

LAUB, J. H., & SAMPSON, R. J. (1993). TURNING POINTS IN THE LIFE COURSE: WHY CHANGE MATTERS TO THE STUDY OF CRIME. *Criminology (Beverly Hills)*, *31*(3), 301–325. https://doi.org/10.1111/j.1745-9125.1993.tb01132.x

Lee, J., Menard, S., & Bouffard, L. (2013). Extending Interactional Theory: The Labeling Dimension. Deviant Behavior, 35(1), 1–19. https://doi.org/10.1080/01639625.2013.822208

Lee, S. (2003). Testing Thornberry's interactional theory: The reciprocal relations. ProQuest Dissertations Publishing.

Lerner, J., & Tirole, J. (2002). Some Simple Economics of Open Source. Journal of Industrial Economics, 50(2), '97-234.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the "cryptomarket." Criminology & Criminal Justice, 14(3), 351–367. https://doi.org/10.1177/1748895813505234

May, T., & Hough, M. (2009). Drug markets and distribution systems. Addiction Research & Theory. 12. 549-563. 10.1080/16066350412331323119.

Meyer, C. B. (2001). A case in case study methodology. Field Methods, 13, 329–352.

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study. Security Journal, 32(2), 102–118. https://doi.org/10.1057/s41284-018-0150-5
Moore, D. & Rid, T. (2015), "Cryptopolitik and the Darknet," Survival, vol. 58, no. 1

Moore, D., and T. Rid. (2016). Cryptopolitik and the Darknet. *Survival* 58 (1): 7–38.

Morse J.M., Field P.A. (1996) The purpose of qualitative research. In: Nursing Research. Springer, Boston, MA. https://doi.org/10.1007/978-1-4899-4471-9_1

Moore, D., and T. Rid. 2016. Cryptopolitik and the Darknet. *Survival* 58 (1): 7–38.

Owen, G., & N. Savage. (2015). *The tor dark net*, 20. Paper Series no: Global Commission on Internet Governance.

Owenson, G., Cortes, S., & Lewman, A. (2018). The darknet's smaller than we thought: The life cycle of Tor Hidden Services. *Digital Investigation*, *27*, 17–22. https://doi.org/10.1016/j.diin.2018.09.005

Pace, J. (2017). Exchange Relations on the Dark Web. *Critical Studies in Media Communication* 34 (1): 1–13.

Patricia Bazeley. (2018). Inherently Mixed, Hybrid Methods. In *Integrating Analyses in Mixed Methods Research* (p. 235–). SAGE Publications Ltd. https://doi.org/10.4135/9781526417190.n10

Patulny, R. (2005). Social rights and social capital: Welfare and co-operation in complex global society. Australian Rev Public Aff. 6.

Paoli, G. P., Aldridge, J., Nathan, R., & Warnes, R. (2017). Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.

Preece, J., Rogers, Y., & Sharp, H. (2002). Interaction Design: Beyond Human-Computer Interaction. New York: John Wiley & Sons.

Quintin, C., (2014), 7 Things You Should Know About Tor, Electronic Frontier Foundation, July 1, 2014.

Qiang; Zhao, Yue; Ye., & Li, Ziru. (2014)."The Relationship between Online Attention and Share Prices" *WHICEB 2014 Proceedings*. 2.https://aisel.aisnet.org/whiceb2014/2

**Raab, C. (2017), 'Security, Privacy and Oversight', pp. 77-102 in Andrew Neal (ed.), Security in a Small NaBon: Scotland, Democracy, PoliBcs. Cambridge: Open Book Publishers.**

Rudesill, D.S., Caverlee, J. and Sui, D. 2015. The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Ohio State Public Law Working Paper No. 314.

Röttger-Rössler, B., Scheidecker, G., Funk, L., & Holodynski, M. (2015). Learning (by) Feeling: A Cross-Cultural Comparison of the Socialization and Development of Emotions. *Ethos (Berkeley, Calif.)*, *43*(2), 187–220. https://doi.org/10.1111/etho.12080

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. doi:10.1080/21931674.2014.991184

**Sampson, R. J. and J. H. Laub. 1993 Crime in the Making: Pathways and Turning Points through Life. Cambridge M.A.: Harvard University Press.**

**Sampson RJ and Laub JH (2003) Life-course desisters? Trajectories of crime among delinquent boys followed to age 70. Criminology, 41(3): 555–592**

Schneier, B. (2013). "Attacking Tor: How the NSA Targets Users' Online Anonymity," The Guardian, October 4, 2013.

Seddig D (2013) Crime inhibiting, interactional and co-developmental patterns of school bonds and the acceptance of legal norms. Crime and Delinquency (in press).

*Shillito, M. (2019). Untangling the "Dark Web": an emerging technological challenge for the criminal law. Information & Communications Technology Law, 28(2), 186–207. https://doi.org/10.1080/13600834.2019.1623449*

Spitters, M., Verbruggen, S., & Staalduinen, M. V. (2014). Towards a comprehensive insight into the thematic organization of the Tor hidden services. Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint (pp. 220–223). IEEE

*Stalans, L. J., & Finn, M. A. (2016). Understanding how the internet facilitates crime and deviance. Victims & Offenders, 11(4), 501-508. doi:10.1080/15564886.2016.1211404*

Soska, K. and Christin, N. 2015. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. Proceedings of the 24th Usenix Security Symposium; 12–14 August 2015, Washington, D.C: Advanced Computing Systems Association.

Tanenbaum, A., & Van Steen, M. (2007). Distributed systems : principles and paradigms (2nd ed.). Pearson Prentice Hall.

The Tor Project. (2018). Users. https://metrics.torproject.org/userstats-relay-country.html. Accessed 3 February 2018.

Terence P. Thornberry. (2005). Explaining Multiple Patterns of Offending across the Life Course and across Generations. The Annals of the American Academy of Political and Social Science, 602(1), 156–195. https://doi.org/10.1177/0002716205280641

*Thomas, K. (2015), Framing Dependencies Introduced by Underground Commoditization.*

Thomaz, F., Salge, C., Karahanna, E. *et al.* Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *J. of the Acad. Mark. Sci.* 48, 43–63 (2020). https://doi.org/10.1007/s11747-019-00704-3

*THORNBERRY, T. (1987). TOWARD AN INTERACTIONAL THEORY OF DELINQUENCY. Criminology (Beverly Hills), 25(4), 863–892. https://doi.org/10.1111/j.1745-9125.1987.tb00823.x*

Thornberry, T. (1986). "The Effects of Consequences on Patterns of Social Interaction: A Quasi-Experimental Approach to Reinforcement in Natural Interaction." Child Development 57: 1257-1268.

Thornberry, T. P. 1997."Introduction: Some Advantages of Developmental and LifeCourse Perspectives for the Study of Crime and Delinquency." In T.P. Thornberry (Eds.), Advances in Criminological Theory, Vol. 7. Developmental Theories of Crime and Delinquency. New Brunswick, N.J.: Transaction Publishers.

Thornberry T. P., A. J. Lizotte, M. D. Krohn, M. Farnworth, S.J. Jang. 1994. "Delinquent Peers, Beliefs, and Delinquent Behavior: A Longitudinal Test of Interactional Theory." Criminology 32:47-83

Thornberry., T & Krohn., M, (2005) . "Applying Interactional Theory to the Explanation of Continuity and Change in Antisocial Behavior . Pp. 183 – 210 in *Integrated Developmental and Life-Course Theories of Offending: Advances in Criminological Theory* , Vol. 14 , edited by P. David , Farrington. New Brunswick , NJ : Transaction .

Thornberry, T. (1991). "Testing Interaction Theory: An Examination of Reciprocal Causal Relationship among Family, School, and Delinquency." Journal of Criminal Law and Criminology 82:3-35.

Van Hout, M. C., & Bingham, T. (2013). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *The International Journal of Drug Policy*, *25*(2), 183–189. https://doi.org/10.1016/j.drugpo.2013.10.009

Warr M (1993) Age, peers and delinquency. Criminology, 31(1): 17–40.

Warr M (2002) Companions in Crime: The Social Aspects of Criminal Conduct. Cambridge: Cambridge University Press.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict and Terrorism*, *39*(3), 195–206. https://doi.org/10.1080/1057610X.2015.1119546

Weerman FM (2011) Delinquent peers in context: A longitudinal network analysis of selection and influence effects. Criminology, 49(1): 253–286.

Wegberg, R. (2018). Plug and prey? measuring the commoditization of cybercrime via online anonymous markets.

Winker, I., & Gomes, A. (2016). Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies. https://www.elsevier.com/books/advanced-persistent-security/winkler/978-0-12-809316-0

Wollebæk, D., Karlsen, R., Steen-Johnsen, K., & Enjolras, B. (2019). Anger, Fear, and Echo Chambers: The Emotional Basis for Online Behavior. Social Media + Society, 5(2), 205630511982985–. https://doi.org/10.1177/2056305119829859

Yarbrough, A., Jones, S., Sullivan, C., Sellers, C., & Cochran, J. (2012). Social Learning and Self-Control: Assessing the Moderating Potential of Criminal Propensity. International Journal of Offender Therapy and Comparative Criminology, 56(2), 191–202. https://doi.org/10.1177/0306624X10396041

Yin, R. K . (1994). Case study research: Design and methods. Beverly Hills, CA: Sage.

Yus, F. (2011). Cyberpragmatics Internet-mediated communication in context . John Benjamins Pub. Co.