June 2022

Cryptrust: The Role of Trust Between Buyer and Vendor on Dark Web Firearms and Drug Markets

Richard Frank, Noelle Warkentin, Yuxuan (Cicilia) Zhang, and Shu Qi Liu

International CyberCrime Research Centre (ICCRC)
Simon Fraser University

BRITISH COLUMBIA Ministry of Public Safety and Solicitor General
Royal Canadian Mounted Police Gendarmerie royale du Canada
SFU SIMON FRASER UNIVERSITY

Table of Contents

List of Tables

List of Figures

The Crime Reduction Research Program

This project was funded through the British Columbia Crime Reduction Research Program (CRRP).

The CRRP is a research grant program administered and funded by the Province of British Columbia in collaboration with the Royal Canadian Mounted Police (RCMP). The CRRP is focused on investing in independent research to inform priority policing operations, policies, and programs related to public safety in British Columbia. In doing so, the CRRP also aims to foster greater collaboration between government, law enforcement, and academic experts in the field of policing and public safety.

Eligible research topics are identified on an annual basis by the BC Ministry of Public Safety & Solicitor General and the RCMP based on current and emerging provincial priorities. All grants are awarded on a merit basis by the CRRP Working Group.

Disclaimer

Abstract

Cyber-enabled crimes are becoming more prevalent, leading to an evolution of the illicit firearms and drug trafficking landscape. For this reason, it is crucial to determine the characteristics of trust the most successful offenders employ within dark web illicit firearms and drug markets as a means to assist law enforcement to identify and prioritize these types of targets. Whereas the vast majority of previous research on illicit cryptomarkets have focused on the products or the marketplaces on the dark web, research on the people – their social interactions and demographic behaviour – is still in its infancy. The current study aimed to extend the methodological framework of measuring consumer trust in the online illicit drug trade developed by Kiss, Parti, and Prazsák (2019) for the illicit firearms cryptomarkets. Using a set of surveys, one aimed towards darknet market users, and one aimed towards university students, we assessed which trust factors based on specific scenario questions were most important in the purchasing of illicit goods online. Results indicate that there is a difference in responses from the two samples surveyed, as only those in the university sample with specific expertise differed in responses compared to those who lacked specific expertise. In contrast, having specific expertise did not influence responses in the sample of darknet users. Lastly, while only two of our research questions yielded consistent reporting between the two populations, results from this study have aided in our understanding of trust mechanisms at play within these darknet markets.

Keywords: Darknet markets; Cryptomarkets; Firearms; Drugs; Trust; British Columbia

Acknowledgements

We gratefully acknowledge the financial support of the Crime Reduction Research Program, administered in partnership between the Ministry of Public Safety and Solicitor General, the Combined Forces Special Enforcement Unit of British Columbia, and RCMP ‘E’ Division.

Chapter 1. Introduction

Cyber-enabled crimes are becoming more prevalent, and are quickly evolving the illicit firearms and drug trafficking landscape. While criminological and behavioural economic theory support this paradigm shift (Becker, 1974; Cornish & Clarke, 1986; Cohen & Felson, 1979; Thibaut & Kelley, 1959), there remains a gap in the available data to illustrate a model for targeting individuals and informing police target prioritization. In 2017, researchers with the RAND Corporation found that of 811 arms related listings, illicit firearms, including those potentially diverted from legal owners, accounted for 42% of the market share (Paoli, Aldridge, Ryan, & Warnes, 2017). For the same year, the United Nations Office on Drugs and Crime estimated that drug trafficking accounted for 62% of all illicit online transactions (UNODC, 2020a). Online transactions involve both the clear web (using encrypted communication) and the dark web, which forms part of the deep web. In order to access the dark or the deep web, regular browsers cannot be used, and instead users must access them using anonymizing software (Botsman, 2017). The first anonymizing software, an encrypted network known as The Onion Router (Tor), was released by researchers in 2002 (Dingledin, 2002). This network provided anonymity to users, allowing some individuals to use this to their advantage by creating websites for illegal activity, such as online marketplaces known as cryptomarkets. It is within these cryptomarkets that the sale of illicit firearms and drugs are being distributed, as there are no legal regulations controlling the transactions within these markets (Botsman, 2017).

With an influx of individuals moving online to sell illicit goods, it becomes important to understand the scope of buyers and vendors transitioning from traditional illicit firearms and drug trafficking to the dark web. Since Cryptomarkets and the dark web afford their users greater physical security, lower operational costs, and reduced risk of arrest, there is little in the way of preventing the move to these darknet markets. In many cases, these modalities also enable individuals to operate independently from large criminal organizations, and often exploit licit supply chains. While offenders were originally thought to have been primarily motivated by the physical safety of conducting transactions online, the motivations are now much more dynamic. Since these darknet markets provide the opportunity for anonymity, those who may not have committed criminal offences in person may now choose to facilitate such criminal activities in these spaces, especially as facilitation by tech-savvy straw persons becomes more commonplace (UNODC, 2020b). Therefore, it is crucial to determine which trust factors the most successful offenders employ within dark web illicit firearms and drug markets, as a means to assist law enforcement to identify and prioritize the characteristics of these targets.

Chapter 2. Cryptomarkets

Cryptomarkets are online marketplaces that use encrypted internet protocols (for example, Tor) and rely on cryptocurrencies such as Bitcoin, Monero, and Ethereum. Each transaction on a cryptomarket is between two parties—buyer and vendor—who are connected by shared trust fortified by information communication technology (Botsman,

2017). Vendors using the site are charged a certain percentage by the cryptomarket (Christin, 2013; Martin, 2013) as the cryptomarkets provide a level of security and trustworthiness for the vendor. Not only are cryptomarket owners responsible for evading law enforcement, but they must also prevent scams, while allowing for the facilitation of transactions (Morselli, Giguere & Petit, 2007; Lane, Lacey, Stanton, Matthews, & Salmon, 2018).

In order to prevent scams, cryptomarkets often use the escrow system, in which the market will hold the money until the buyer has received the product (Bradley, 2019). This protects both the vendor and the buyer; once the buyer receives the product the money is released to the vendor, or in the case of products not being shipped, buyers are reimbursed from the market. In any instances of disputes between the vendor and the buyer, market administrators will be the judge of who keeps the money. A “finalize early” option is otherwise provided, in which the vendor is paid directly before the order is even delivered. Some markets, to mitigate vendors taking money without shipping the product (known as an exit scam), require vendors to pay bonds in order to operate in that market. The cost of the bond deters those looking to scam since the operating cost to sell within the market usually outweighs any profit they would acquire from a scam. In the case that a vendor does get banned from a market they must repay the bond before they can operate within that market again.

The security of cryptomarkets are so strong that they are extremely resilient against interdictions from law enforcement as well as attacks against its ecosystem (Bradley, 2019; Buskirk, Bruno, Dobbins, Breen, Burns, Naicker, & Roxburgh, 2017; Decary-Hetu & Giommoni, 2016). This security is provided by the fact that when accessing these sites (through Tor or I2P), the device will be connected through a random path of other networked devices to the server, therefore making it difficult for law enforcement to identify website hosts, as well as who is visiting them (Bradley, 2019). In fact, following the investigation led by FBI and Europol (known as Operation Onymous), as well as the Evolution market exit scam, cryptomarkets were able to recover quickly, and sales were not impacted greatly (Decary-Hetu & Giommoni, 2016). Factors that were found to decrease individual users’ resilience were: Loss of reputation, access to their account, as well as method of communication with buyers and partners (Bradley, 2019). Cryptomarkets and users were both found to be resilient to financial losses (Bradley, 2019), possibly because the effort and time spent building a reputation would be more difficult to recover compared to the financial impact.

2.1. Trust in Cryptomarkets

In the entrepreneurial world trust is essential, not only in reducing risks, but also in governing relationships (Welter, 2012). While this applies to the licit entrepreneurial world, it also applies to those entrepreneurs within the illicit world, such as cryptomarkets. Trust is reciprocal in a relationship, with risks to the vendor in regards to law enforcement, as well as the buyer who not only considers risk with law enforcement, but must also trust the vendor with price and product quality (Tzanetakis, Kamphausen, Werse, & von

Laufenberg, 2016). With the anonymity offered by cryptomarkets, therein lies the risk of self-serving behaviours, where individuals act to their own benefit and sometimes at the expense of others (Linder, 2019). Since buyers do not know the identity of the vendor, the only way they can distinguish between vendors is by their online username, and from the person-specific encryption keys the vendor uses to encrypt their messages (Broseus, Rhumobarbe, Mireault, Ouellette, Crispino, & Decary-Hetu, 2016). By default, there is zero trust between the buyer and vendor; however, cryptomarkets have attempted to solve this through trust in the platform; instead of relying on vendors and buyers building trust with each other first, trust can initially be established with the cryptomarket, as this can be the go-between for each party to ensure completed transactions. The strengthening of horizontal trust has had a significant impact on the functioning of illicit cryptomarkets and has aided the organization of self-regulated online communities capable of supporting illicit trade without trust or external regulation. This has been accomplished despite law enforcement and regulatory pressures to eradicate them. The perceived anonymity and convenience of the dark web and cryptocurrencies allow offenders to complete these transactions easily, while broadening their market base, all without explicit trust.

Prior research aimed at investigating trust within online drug markets have identified two strong factors relating to trust between buyers and vendors: The reputation of the vendor, and past experiences a buyer has had with the vendor (Norbatus, Ruiter, & Corten, 2020a; Linder, 2019; Norbatus, Ruiter, & Corten, 2020b). In a study conducted by Tzanetakis et al. (2016) the authors qualitatively analyzed customer feedback and profile pages of four drug trafficking vendors within the Agora cryptomarket. The authors found that vendor profiles contributed to building trust, as they listed reviews, information about refunds, as well as an overall rating from previous buyers. In addition, they found that vendors built trust through posting on forums, which gave buyers the opportunity to connect with the vendor and read informal reviews about others experiences (Tzanetakis et al., 2016). Thus, in addition to the information provided on vendor sites, it was the reputation from informal reviews in conjunction with rating systems that aided in establishing trust.

Similarly, Norbatus et al. (2020a) analyzed buyer feedback messages within a known drug cryptomarket to determine whether buyers relied more on past experiences or on reputation based on others' reviews. The authors found that although a buyer does consider the reputation of a vendor in their purchasing decision, the buyers' own history with that specific vendor is a better indicator of future purchasing behaviour. In addition, in their research on reputation transferability within cryptomarkets, Norbatus et al. (2020b) found that those vendors who have a longer history with a good reputation often continue to use the same identity across markets. Since they have built their reputation on the basis that others can trust their products and service, they maintain this reputation across markets by carrying over their identity[1]. These findings highlight the importance of reputation, as this factor not only improves trust with continued interactions, it accelerates trust into additional markets (Norbatus et al., 2020b).

[1] Vendors may sell their products/services across multiple cryptomarkets.

While the previous studies aimed at understanding trust with drug vendors in cryptomarkets, another recent study investigated how trust is formed for the firearm vendors within cryptomarkets. Copeland, Wallin and Holt (2019) qualitatively analyzed six vendors who specifically sold weapons within cryptomarkets to understand vendor practices, including weapons sold, product price, and how trust is gained. The authors found that the information displayed on the vendors' sites, including product photos, shipping details, and escrow information, all supported trust with potential buyers (Copeland et al., 2019). Some vendors also offered specific details about how to avoid detection by authorities when the item is shipped, which further aided in building trust with buyers (Copeland et al., 2019). In addition to providing specifics about products and shipping, trust was established by reviews about the vendor, which supported their reputation, as well as by the vendor sharing some personal information (Copeland et al., 2019). These findings extend the current knowledge on how trust is built within the cryptomarket environment. While reputation and previous buyer experience are important factors in building trust in these relationships, specific details such as how to avoid detection, and personal elements are also contributing factors.

2.2. The Current Study

The current study will extend the methodological framework of measuring consumer trust in the online illicit drug trade developed by Kiss, Parti, and Prazsák (2019)[2], to the illicit firearms sold within cryptomarkets. From ongoing research in the fields of cryptomarkets and cyber-enabled crime, the study will make use of The Dark Crawler[3], a web-intelligence tool developed by the Principal Investigator, to identify active illicit firearms and drug cryptomarkets and collect vendor profile information (Frank, 2020).

Rather than survey the *products* on these marketplaces, the aim of this study is to survey the *buyers* and *vendors* on active dark web firearms and drug markets. In this way, we aim to articulate the system of consumer trust which plays a significant role in illicit online transactions, and the behavioural, economic, and technological factors influencing the decision making between them. Whereas the majority of previous research on illicit cryptomarkets have focused on the products or the marketplaces on the dark web, research on the people – their social interactions and demographic behaviour – is still in its infancy. With respect to operational benefits, the primary research aims will be the data-driven development of a threat assessment tool with an emphasis on assessing buyers and vendors who engage in these types of cyber-enabled crimes, and the threat actors operating in illicit firearms and drug cryptomarkets. The resultant tool will include categories of trust and confidence factors indicated by the survey questionnaire respondents. These indicators will be built into a trust matrix that captures individual

[2] The Principal Investigator maintains a research collaboration with Prof. Tibor Kiss from the National University of Public Service in Budapest, Hungary. Prof. Tibor Kiss has shared with the Principal Investigator his project outline, survey design, and preliminary results of their own study.

[3] The Dark Crawler is a web-based application that can be used to collect and analyze online data.

coercive circumstances, organizational behaviour, communication methods, and technological means which enable buyers and vendors to conduct successful transactions. This research project will be collaborating with the Combined Forces Special Enforcement Unit of British Columbia's (CFSEU-BC) Strategic Research Office (SRO) in order to provide operational benefits to the agency's Anti-Trafficking Task Force (ATTF), Crime Gun Intelligence and Investigations Group (CGIIG), Digital Forensics Unit, and Cyber Operations. In addition, units such as the RCMP's Federal Serious and Organized Crime – Cyber Ops Group (COG) as well as the Undercover Program—in the building of online personas and planning of tactical internet undercover operations—could also benefit from the findings in this study.

Chapter 3. Research Questions

In accordance with the topics and objectives of the proposed study, we aim to address the following six research questions:

RQ$_1$. Do those with greater knowledge of the risk factors of illicit firearms and/or illicit drugs, better knowledge of the legal consequences of illicit firearms and drug use and trafficking, and greater technological expertise consider a higher degree of trust to be important when accessing illicit cryptomarkets than those who have less knowledge?

RQ $_2$. Do individuals prefer to purchase products illegally through online avenues in order to avoid legal repercussions relevant to purchases of drugs or firearms through legitimate means? In addition, during this process are those with greater knowledge in technology, or having expertise in legal consequences around using or trafficking illicit products, more likely to choose the darknet to purchase, in comparison to those who do not have this expertise?

RQ $_{3a}$. Does a stronger compulsion buyers or vendors have to obtain illicit firearms and/or drugs, increase the likelihood they choose to use traditional criminal methods to purchase illicit firearms and/or drugs, and decrease confidence factors they consider necessary when utilizing illicit cryptomarkets?

RQ $_{3b}$. Conversely, do those with greater knowledge of the harmful effects and legal consequences of illicit firearms and drug trafficking, and with more expertise in information technology, computing, and communications technology, require more trust factors to be met in order to initiate and complete their transactions?

RQ $_4$. Do successful transactions increase buyers' discretion in relation to illicit trade and the willingness to repurchase, and facilitate the balancing and gap-filling function of the illicit firearms and drug trades on the Internet?

RQ $_5$. Do buyer and vendor confidence factors of covert and untraceable online transactions have a higher threshold to meet basic conditions for decision making?

Chapter 4. Methods

4.1. Participants

In order to investigate the previously stated research questions, data collection targeted darknet market buyers and vendors. This population could provide information useful for understanding how individuals build trust within these illegal online spaces, as these are the primary actors taking part in these online transactions. In addition to darknet market buyers and vendors, data was also collected from university students to further supplement responses in the event that there were few darknet market survey responses. While the university population may or may not have experience in purchasing within these darknet markets, their inclusion was deemed appropriate since they may be knowledgeable in the purchasing of legal and illicit goods online. Further, university students may have greater knowledge of technology, the effects of drugs, or the legal consequences of purchasing illicit products. Therefore, if individuals from this population give answers that are deemed criminal in certain situations, it can be assumed that others in the same age range, but not in university, may give similar answers. Lastly, because university students are generally easier to access in terms of data collection, it was assumed that gathering data from them would easily contribute to the number of responses for data analysis. While responses from both groups would aid in obtaining a larger number of responses, it would also allow for analysis of any differences between the two populations (see Tibor, Ákos, & László, 2020).

4.2. Materials

Data collection was initiated through two separate surveys, one specifically for darknet market users, and one specifically for the university students. SurveyMonkey was identified at the onset of the study as an appropriate platform for hosting the two surveys, as it is an approved cloud-based online survey service with data centres located in Canada, and meets the requirements of BC's FIPPA legislation. Both surveys included mixed interview methods—structured, closed, contingency, and projective questions—to dynamically assess buyers, vendors, and university students. Questions assessed respondents' internet habits, attitudes towards zero-tolerance policies, and knowledge of illicit firearms and/or drugs. Projective and scenario-based questions adapted from real-life stories were used to assess respondents' reactions by selecting from a finite list of trust factors and reactions (*Appendix A*). Specifically, seven scenario-based questions were posed in the survey developed for the darknet market users (*Appendix B*), whereas five scenario-based questions were developed for the university survey (*Appendix C*). The two extra scenarios posed in the survey for the darknet market users were based on firearms and blueprints. These scenarios were not included for the university student survey as there is a limited possibility that students would be familiar with purchases of these types of products. The outputs from projective and scenario-based questions were thought to characterize the decision-making process of the respondents in critical scenarios, their willingness to act, and any distinguishing qualities between demographic profiles, and/or

buyers and vendors. Finally, a set of general demographic characteristics was elicited, with the invitation for respondents to provide information for validation purposes.

4.2.1. Darknet Market Survey

A list of active and accessible dark web forums, including the forums section on cryptomarkets, was created where there appeared to be a high population of darknet market users. The cryptomarkets were identified in January and February 2021 from four sources, Dark.link, Dark net live, Dread, and a sheet from law enforcement that contained cryptomarket names. The cryptomarkets were examined for active forums that were accessible and showed signs of use. The cryptomarkets with active forums were included in the list of forums. Dark net live and Dark.link were also used to identify other forums. When the forums were accessible, had discussion about cryptomarkets, and posts within the past month the forum was included in the forums list.

An account was created for each forum, and a closed, invitation-only online survey questionnaire was sent out to prospective forum moderators, with a request to post the survey. The first forum contacted was Dread, one of the most popular dark web forums, containing many smaller communities on subforums termed subdread. However, the moderators did not allow us to post the survey, banning the CrypTrust account from the subdread. The next forum was on a cryptomarket that primarily sold cannabis products; they politely refused.

Following these failed attempts, we did not believe that any other forums would allow us to post the survey link, and therefore moved to other ways of recruiting survey participants. Rather than focusing on forums on the dark web, Reddit was chosen as a platform that may contain a relatively similar population to darknet market users. For instance, there are dedicated subreddits for all things darknet related, which may attract individuals who are familiar with, or are interested in using, darknet markets. To identify topics on Reddit related to darknet markets, specific keywords were first searched. Keywords included '*Tor*', '*Dark net markets*', '*Dark web*', '*Cryptomarkets*', and '*White House Market*'. Once the subreddits were identified, they were examined for the type of content they often post. If the content was often related to cryptomarkets or technologies used to access cryptomarkets, they were included. For example, if the subreddit was primarily discussing how to find onion links or operational security surrounding Tor, it would be included.

Four subreddits were selected once it was confirmed that advertisements were allowed to be posted on them. The population on those four subreddits was small, so another population of interest, subreddits with people who have IT, legal, or medical expertise, were identified. There were already two subreddits that focused on IT, and the medical focused subreddits had it against their rules to post surveys, so only those with law expertise were selected. Of the subreddits identified through this selection process, five were deemed as appropriate for survey advertisement. The five subreddits selected to promote the survey included: '*onions*', '*tor*', '*darknetdiaries*', '*duckduckgo*', and '*legal*' (see *Table 4.1*).

Table 4.1. Subreddits with populations targeted in advertisements.

Subreddits	Population of Interest
onions	Dark net users
tor	Dark net users and individuals with IT expertise
darknetdiaries	Dark net users
duckduckgo	Dark net users and individuals with IT expertise
legal	Individuals with legal expertise

Formal Reddit advertisements were created and ran from July 31st to September 5th 2021, and from November 10th to November 28th, 2021. The first advertisement was run at the start of the study, targeting only residents of British Columbia; unfortunately, a lack of respondents to this survey meant that targeting only British Columbian residents may be too strict of a pool. For this reason, the second advertisement was run in November, targeting an international audience rather than just those residents of British Columbia. The advertisement was stopped once users were no longer filling out the survey after clicking on it.

4.2.2. University Survey

A total of six universities within British Columbia were contacted for dispersion of the study's survey: University of British Columbia, Simon Fraser University, the University of Victoria, Kwantlen Polytechnic University, Royal Roads University, and Vancouver Island University. Initially, a graduate research assistant emailed letters to departmental deans, describing the survey (with a link to the survey included) and asking for permission to disperse the survey link to department instructors. Specifically, deans from the departments of health sciences, social sciences, and legal studies were contacted for survey dispersal. The first round of emails was sent to 19 deans from the previously listed six universities in July of 2021. This initial round of emails resulted in only three responses, one from Simon Fraser University, and two from the University of Victoria, allowing instructors to be contacted with a link to the survey to distribute to their classes. Because of the limited success in distributing the survey, it was decided that a second round of emails would be sent out in the following term. In October 2021, the same 19 departmental deans from the same universities were again contacted with the same letter asking for permission, and with a link to the survey. From this second round, only one (from Simon Fraser University) agreed to allow the survey to be distributed. For the most part, the majority of deans contacted did not respond at all, and the ones that did decline usually stated that their students were too busy, or that they were not comfortable with the survey being distributed.

4.3. Data Cleaning

Prior to working with the survey data, individual responses from each survey were downloaded from SurveyMonkey into an .XLSX format. This produced two new Excel documents, one for the Darknet Market survey, and one for the University Survey. Originally, the Darknet Market survey contained 222 individual responses, and the University survey contained 74. However, upon data cleaning, these numbers were drastically reduced.

To begin, each dataset was read through to identify any instances of missing data, and each dataset was cleaned based on these findings. Within the Darknet Market survey, participants who had not consented, and therefore had not completed any of the survey questions, were removed from the dataset. In addition, participants from both surveys were removed from the datasets if they had stopped responding after the initial consent, or if they had not responded past answering how often they had shopped online. Since this was one of the first questions in both surveys, a lack of responses following this question meant that participants had not taken part in any of the legal or illegal scenario questions. Since the scenario questions were by far the most important in answering the hypotheses set forth in this study, zero participation in any of these scenario questions would render the participants prior answers useless. In the end, the Darknet Market survey yielded 101 participants for analysis[4], while the University survey yielded 55 participants for analysis (see *Figures 4.1* and *4.2*).

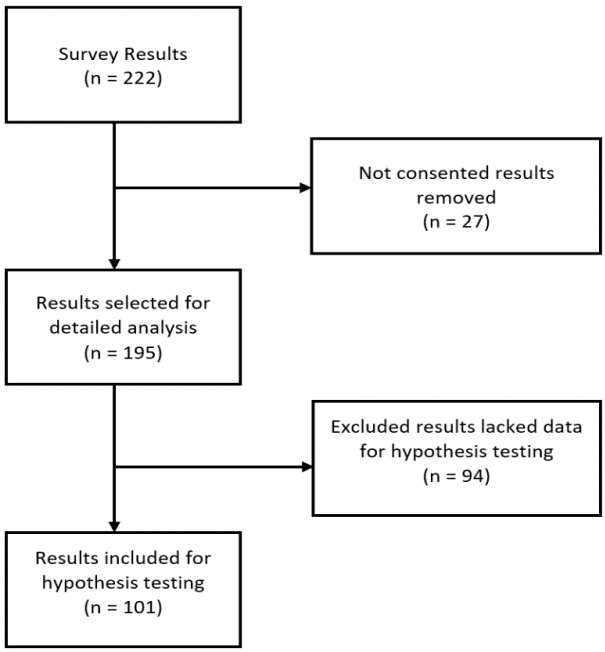

Figure 4.1. Data cleaning method for the Darknet Market survey.

[4] Although this leaves a relatively small sample for results, this still provides some understanding from those who did respond.

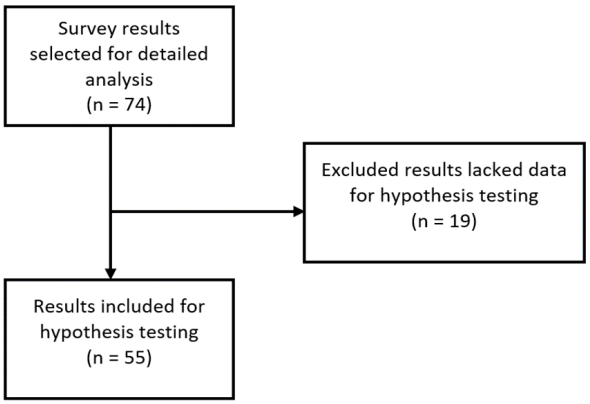

Figure 4.2. Data cleaning method for the University survey.

4.4. Data Analysis: Research Questions

In order to confidently answer each of the research questions set forth in this study, data analysis was completed separately for each of the hypotheses. Since different survey questions were involved with each, or variations of each question, differing analysis techniques had to be applied. The methods used for each hypothesis is described in detail below[5].

4.4.1. Research Question One

Do those with greater knowledge of the risk factors of illicit firearms and/or illicit drugs, better knowledge of the legal consequences of illicit firearms and drug use and trafficking, and greater technological expertise consider a higher degree of trust to be important when accessing illicit cryptomarkets than those who have less knowledge?

To properly answer this research question, respondents from both surveys who answered that they had greater knowledge in information technology, effects and applicability of illicit drugs and/or firearms, or legal and criminal consequences of using or trafficking illicit products needed to be separated out from those who did not. Since there were four potential answers respondents could give for these questions (see *Table 4.2*), answers needed to first be dichotomized into those who either have greater knowledge, or those who do not. Therefore, the two responses (*Yes, because this relates to my work/profession* and *I have a higher than average expertise in this area, but am not an expert yet.*) were transformed to '*yes*'. As well, the two responses (*I am informed about this field but am not an expert. This knowledge is not within my field of work or studies.* and *I have no expertise and do not know about…*) were transformed to '*no*'. Answers for all participants who answered *'yes'* were then copied into a new sheet, so their answers to the trust factors in each scenario could be calculated. Again, since there were four responses respondents could give for

[5] A detailed breakdown of survey questions used to answer each hypothesis is available upon request.

these trust factors (see *Table 4.2*), they were also dichotomized as either *'yes'* (*Absolutely required!* and *Very important*), or *'no'* (*Slightly important* and *Not important*). This same method was also employed on those respondents who were dichotomized to the *'no'* (not having expertise in those three fields).

Once the percentages of *'yes'* (the trust factor is important) and *'no'* (the trust factor is not important) were calculated over each scenario, averages for each trust factor across each scenario were calculated. This was done separately for those who have expertise in the three mentioned areas, and those who do not have expertise. This was also done separately between the two surveys. In the end, the averages for each trust factor across each scenario was calculated for all respondents in the Darknet market survey who had expertise, and for those who did not. This was also calculated in the University study for those who had expertise and those who did not. Averages were then compared across both groups (the Darknet market and University surveys compared separately).

Table 4.2. Breakdown of answers that could be given to those questions about expertise and trust factors, along with how each was dichotomized.

Expertise Answers	Answers	Dichotomized
Yes, because this relates to my work/profession.	Absolutely required!	Yes
I have a higher than average expertise in this area, but am not an expert yet.	Very important	Yes
I am informed about this field but am not an expert. This knowledge is not within my field of work or studies.	Slightly important	No
I have no expertise and do not know about...*	Not important	No

**Note: This sentence was finished depending on which of the three areas of expertise was being answered.*

4.4.2. Research Question Two

Do individuals prefer to purchase products illegally through online avenues in order to avoid legal repercussions relevant to purchases of drugs or firearms through legitimate means? In addition, during this process are those with greater knowledge in technology, or having expertise in legal consequences around using or trafficking illicit products, more likely to choose the darknet to purchase, in comparison to those who do not have this expertise?

Respondents who answered that they had greater knowledge in information technology, or the legal and criminal consequences of using or trafficking illicit products were compared with those that did not have greater knowledge in these two fields. Specifically, these two differing subpopulations were compared on the two trust factors. The two trust

factors that were used for this analysis were "*if you had the option of purchasing online or in-person, where would you rather buy it from?*" and "*would you prefer an in-person meeting or online instead? You can suggest other options!*". The same method of dichotomization for these questions was used as in the methods for the first hypothesis (see *Table 4.2*). Once percentages of *'yes'* and *'no'* had been calculated for these two questions for those with and those without expertise, the percentages were averaged across scenarios. Since the latter question had an open-ended portion, respondents could leave their own comments. To analyze this portion of the question, all respondent answers were gathered (separately for each survey) and inductively coded to understand any themes that emerged. This qualitative portion was analyzed separately by two graduate research assistants, and then compared to come to a decisive conclusion. This method was completed individually for those respondents of the university survey, and those from the darknet survey.

4.4.3. Research Question Three (a)

Does a stronger compulsion buyers or vendors have to traffic illicit firearms and/or drugs, increase the likelihood they choose to use traditional criminal methods to purchase illicit firearms and/or drugs, and decrease confidence factors they consider necessary when utilizing illicit cryptomarkets?

Since this hypothesis is based on respondent answers for scenarios, where the urgency of the life situations differed from less urgent to very urgent, only those percentages of *'yes'* (previously dichotomized—see research question one methods) were compared across scenarios. For the University survey these were ordered from most urgent (Karolina, medicine) to least urgent (Henry, marijuana); for the Darknet market survey these were ordered from most urgent (Karolina, medicine) to least urgent (Jack, blueprints). In addition, the two trust factors *"if you had the option of purchasing online or in-person, where would you rather buy it from?*" and "*would you prefer an in-person meeting or online instead? You can suggest other options!*" were compared across each scenario. The same methods employed in the methods for hypothesis 2 were used, except this time the entire population for each survey were gathered, rather than separating those with and without expertise.

Themes were again inductively coded for the open-ended question, combining all scenarios together. Since there were too few open-ended answers within each scenario, it would prove difficult to attempt to identify themes within each scenario for comparison. By combining answers across all scenarios, we can get a better understanding of the major themes that present from all individuals. Since we had previously inductively coded the answers from these questions in the second research question, but with answers separated for those with and without expertise, we were able to use some of the same themes previously found. Since, however, this question required answers from all respondents, some new themes emerged that were not found in the previous hypothesis. This method was completed individually for those respondents of the University survey, and those from the Darknet survey.

4.4.4. Research Question Three (b)

Conversely, do those with greater knowledge of the harmful effects and legal consequences of illicit firearms and drug trafficking, and with more expertise in information technology, computing, and communications technology, require more trust factors to be met in order to initiate and complete their transactions?

Respondents who answered that they had expertise in all of the three fields (not just one or the other) were singled out for analysis, and their answers regarding the trust factors across all scenarios were compared. This required the same dichotomization of answers for the trust factors as discussed in the first research question, as there needed to be an identification of whether or not respondents found the trust factor to be important in their decision to purchase online. Once percentages of how many respondents found each trust factor important and not were calculated, each factor was averaged across all scenarios. Averages for each trust factor in the illegal scenarios were then compared to responses from the legal scenario, to gauge if there was any difference in how important each trust factor was. This method was completed individually for those respondents of the University survey, and those from the Darknet survey.

4.4.5. Research Question Four

Do successful transactions increase buyers' discretion in relation to illicit trade and the willingness to repurchase, and facilitate the balancing and gap-filling function of the illicit firearms and drug trades on the Internet?

Each illegal scenario contained a question asking the respondent that if they had a successful first transaction "*would you buy from the vendor in a similar situation?*". This question was used to answer this fourth research question. There were three potential answers to this question: *Yes, no*, and *I don't know.* The percentages of each answer were calculated for this question within each of the scenarios separately. Results were then graphed to depict how answers varied across the different scenarios. This method was completed individually for those respondents of the University survey, and those from the Darknet survey.

4.4.6. Research Question Five

Do buyer and vendor confidence factors of covert and untraceable online transactions have a higher threshold to meet basic conditions for decision making?

Lastly, the methodology used for research question five involved comparing the category of trust factors related to secrecy and anonymity between the illegal scenarios, and the legal scenario. There were three trust factors within this category: Opportunity to buy in a hidden and untraceable way, my purchase information should be deleted immediately, and my real details should not even be known to the vendor. First, as had been previously done (see methods for research question one) answers for each question were dichotomized into *'yes'* or *'no'*. Following this, percentages of yes responses were taken for each of the three factors within each scenario and graphed. This was also conducted on the same questions within the legal scenario. Once percentages of all *'yes'* responses were

calculated, they were graphed to visually compare the percentages of importance between the legal scenario and all illegal scenarios.

Chapter 5. Results

5.1. Descriptives

Prior to answering the set of scenario-based questions, respondents were first asked to answer questions related to their internet habits, attitudes towards zero-tolerance policies, and knowledge of information technology (IT), illicit firearms and/or drugs, and legal consequences of illicit products. For darknet market participants, the majority of them (83%) admitted using internet browsers such as TOR that allow browsing in a hidden way and without their user data being collected. On the contrary, only 29% of the university respondents have used internet browsers that would hide their identity while browsing (*Figure 5.1*).

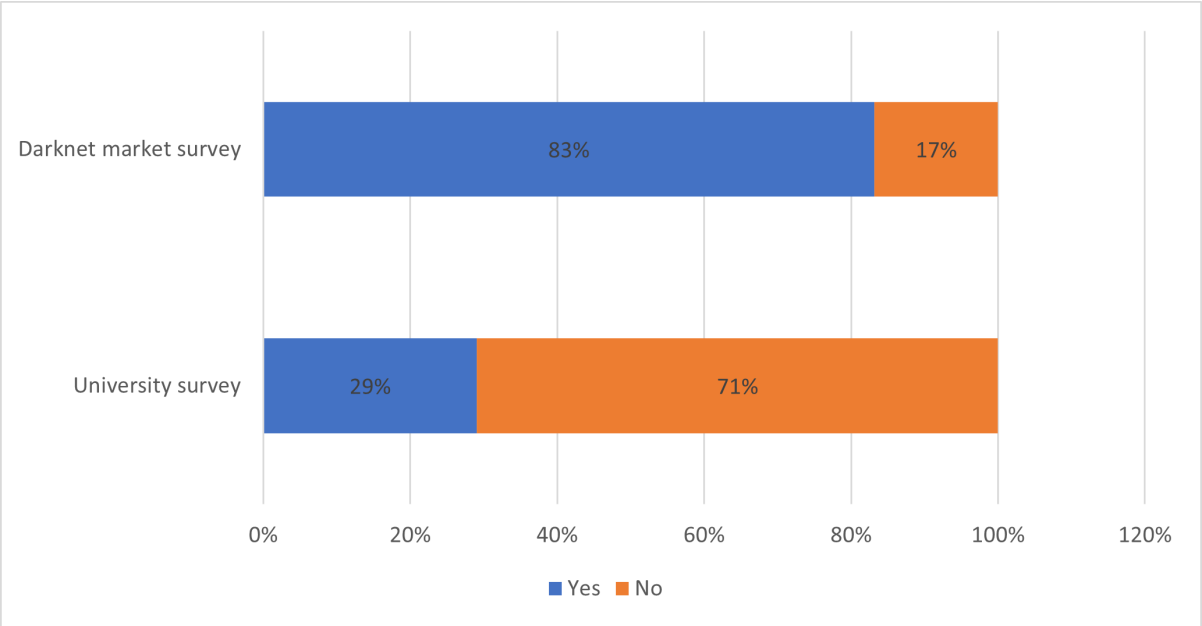

Figure 5.1. Participants' use of internet browsers, aside from private-mode, that do not collect user data or allow browsing using a hidden identity (e.g., TOR browser).

When asked "*what is your level of tolerance towards illicit drugs?",* with 0 representing *there should be no tolerance towards illicit drugs*, and 10 resembling *no drugs should be criminalized*, respondents from the darknet survey have displayed more lenient views toward illicit drugs than university participants. Within the darknet market survey, a significant proportion of the respondents (23%) fully agree with the idea that drugs should not be criminalized, and another 25% of users ranked 8 or 9 for the question, yielding nearly half of the respondents expressing strong tolerance toward illicit drugs. Another five of the respondents (5%) expressed zero-tolerance toward drug use, with a total of

eighteen percent of the respondents (n = 18) marked 0 or 1 or 2 for the question (*Figure 5.2*).

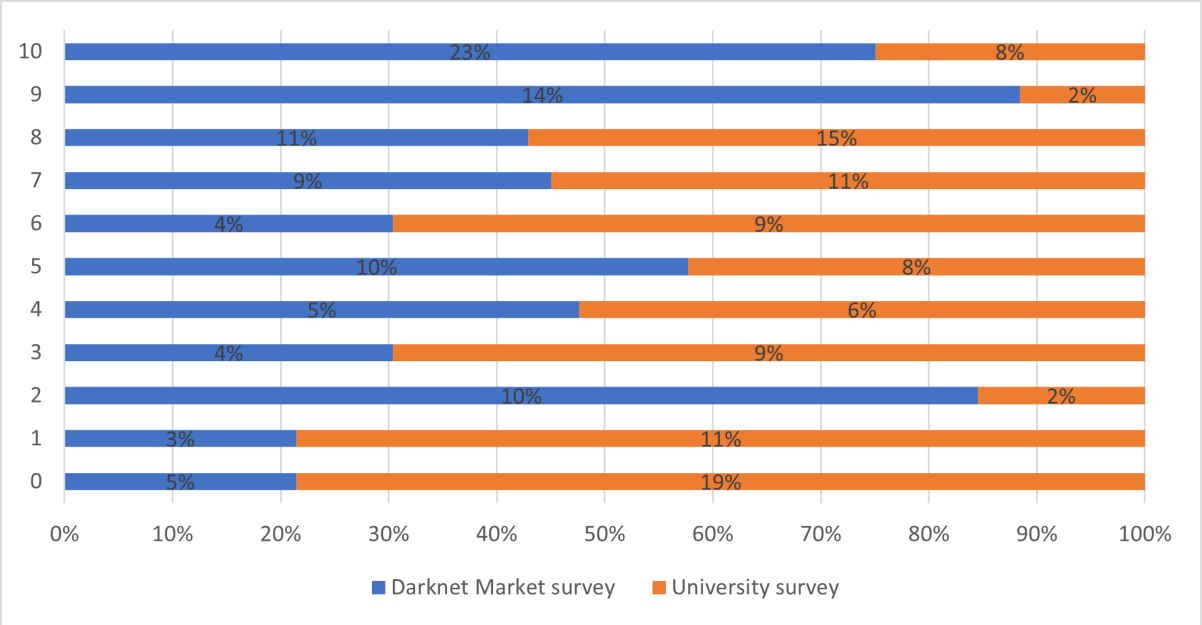

Figure 5.2. Participants' level of tolerance toward illicit drugs.

Different from darknet market users, survey responses from university participants revealed a large proportion of individuals expressing low tolerance toward illicit drugs: 19% of the participants (n = 10) thought there should be zero-tolerance toward drug use, and a total of 32% of them (n = 17) ranked 0 or 1 or 2 for the question. At the same time, thirteen of the participants (25%) supported leniency towards illicit drugs through ranking 8 or 9 or 10 for the question, of which four of them (8%) agreed that no drugs should be criminalized.

We were also interested in respondents' expertise in information technology (IT), effects of illicit drugs and/or firearms, as well as legal consequences related to buying, selling, and trafficking of illicit products. In the darknet market survey sample, 33 of the individuals (33%) identified themselves having skills in IT and technology. A smaller proportion of individuals (9%) identified themselves being experts on the applicability and effects of illicit drugs and/or firearms. In regards to expertise in the criminal or legal consequences of the illegal use and trafficking of firearms and drugs, only 10% of the respondents (n = 10) considered themselves as having expertise in this field. The remaining 49 respondents (49%) in the sample did not identify expertise in any of the three fields (*Figure 5.3*).

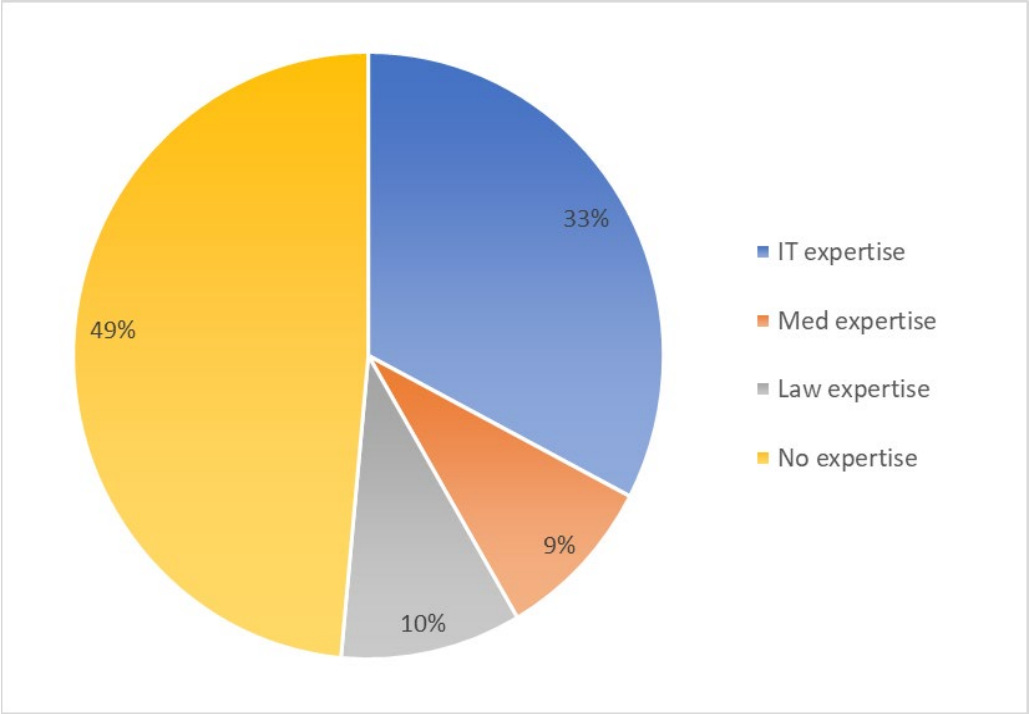

Figure 5.3. Percentage of participants with expertise within the Darknet market survey.

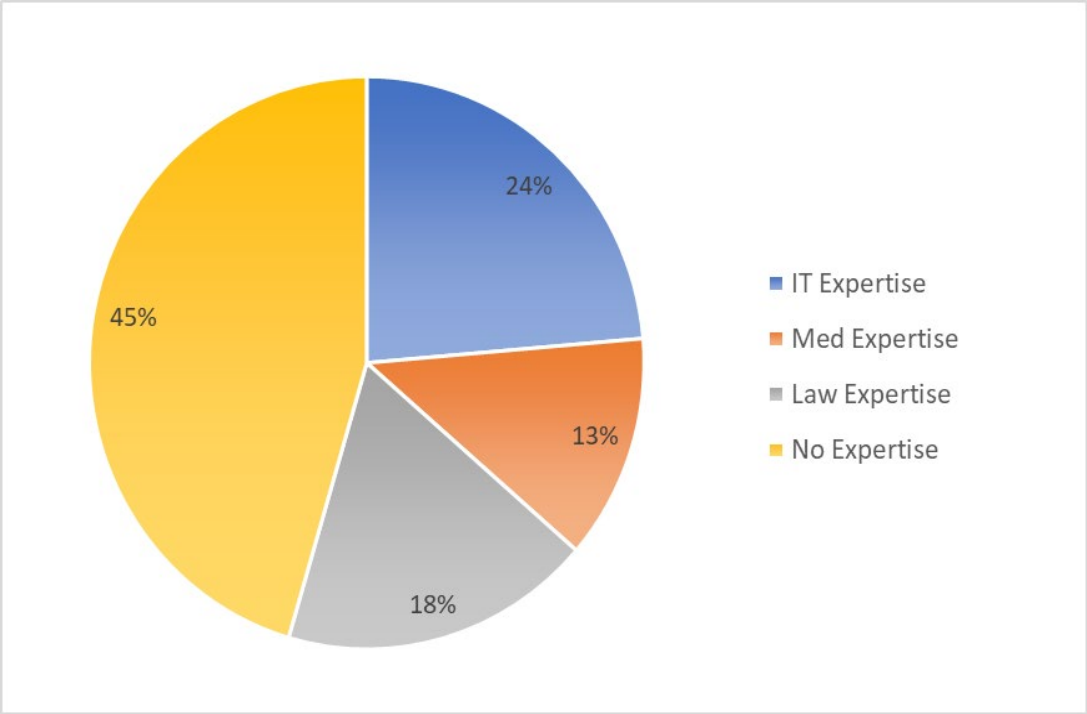

Figure 5.4. Percentage of participants with expertise within the university survey.

As shown in *Figure 5.4* above, almost half of the respondents (45%) in the university survey sample do not consider themselves having expertise in any of the three fields. Out of the

remaining 30 respondents (55%), 24% of them identified themselves having skills within the IT field. A further 13% of the respondents (n = 7) consider themselves having knowledge related to the use, applicability, and trafficking of illicit drugs and/or firearms. Lastly, ten participants (18%) identified themselves as experts in criminal or legal consequences relevant to illicit drugs and/or firearms.

In addition to these descriptives, trust factors from each scenario were aggregated into specific categories, which were based off of the paper that this study is modeled after (see Tibor, Ákos, & László, 2020). The categories are as follows: Individual and community, Technology and network, Data protection and privacy and legal information, Payment transaction, Products and services, Transportation services, and Secrecy and anonymity (see *Appendix A* for a full list of categories). Results were calculated for each trust factor for each scenario by calculating the number of times each response was made for each of the trust factors. Percentages were then gathered for each of these factors, and graphed within each respective category[6].

5.2. Research Question One Examination[7]

For our first research question, we wanted to understand whether individuals with expertise in information technology, the effects and applicability of illicit drugs and/or firearms, or legal and criminal consequences of using or trafficking illicit products will require greater levels of trust when accessing illicit cryptomarkets.

5.2.1. Darknet market survey

For the darknet market survey sample, participants with greater knowledge in computer science, IT, or communications technology are shown to require a higher degree of trust when accessing illicit cryptomarkets than those who do not have technological expertise. Out of the 22 trust factors listed in *Table 5.1*, **users with IT skills ranked thirteen factor categories as more important** when accessing illicit darknet markets. Those with greater knowledge in medicine and the effects of drugs on humans are shown to require a higher degree of trust when accessing illicit cryptomarkets than those who do not have such expertise. When comparing responses between the two groups, **users with expertise on the effects of illegal firearms and drugs considered fifteen trust factors as more important** when making purchases in the illegal cryptomarket than those without skills. When comparing between individuals with or without knowledge related to legal consequences of medicine, criminal law on illicit drug use, or other legal regulations, respondents with greater knowledge required a higher degree of trust than those who do not have such expertise. **Users with expertise on legal consequences and legislations considered twelve trust categories as important** when making an illegal purchase on the darknet under the different scenarios. These trust factors can be seen in the highlighted cells within the expertise group column of *Table 5.1.*

[6] Available upon request.

[7] For a detailed breakdown of results from each hypothesis, see Appendix D.

A number of common and unique trust factors were identified through comparing findings across all expertise and non-expertise groups. Within the darknet survey sample, participants acquiring knowledge in any of the IT, medical, or law field commonly considered five trust factors as very important when accessing illicit cryptomarkets online: **(1) instant response on your online payment transaction; (2) online payment option; (3) accessible, fast and easy payment transaction; (4) the option of registering, or not, for browsing and purchases;** and **(5) protection of personal and purchase data.**

On the contrary, three out of the 22 trust categories were unanimously identified by all expertise groups as not important when purchasing illicit products through cryptomarkets (as comparing to individuals with no expertise): **(1) traditional offline payment option; (2) the popularity and positive feedback of the web store on the internet; (3) the recommendation of the store by acquaintances or friends**. More interestingly, our study results also revealed three important trust factors that were uniquely identified by respondents with IT expertise when purchasing through illicit cryptomarkets. For individuals with IT skills, whether there are **opportunities available to buy illicit products in a hidden and untraceable way, the reliability of goods delivery, as well as the amount of information and details about the prices, goods, and services offered by the vendors** are important factors to consider when purchasing illicit products from the marketplaces.

Table 5.1. Darknet survey: Trust factors considered as important through comparing averages between expertise and non-expertise groups, across all scenarios. Identified important factors by the group are ones with higher percentage and are coloured. Note: [a] non-important trust factors identified by all expertise groups. [b] important trust factors identified by all expertise groups.

Trust Factors	Expertise Groups			Non-expertise Groups		
	IT	Medicine	Law	IT	Medicine	Law
Vendor contact and helpfulness	70.4%	78.1%	74.3%	73.5%	70.2%	71.1%
Vendor reliability	95.5%	94.4%	87.7%	82.7%	88.5%	90.4%
My real details should not even be known to the vendor	79.3%	79.0%	73.7%	70.4%	74.2%	75.1%
My purchase information should be deleted immediately	90.0%	90.8%	85.3%	81.0%	85.1%	86.1%
Opportunity to buy in a hidden and untraceable way	90.9%	82.8%	84.6%	87.9%	91.7%	91.2%
Reliable delivery of goods	94.5%	90.9%	91.1%	92.8%	94.3%	94.1%
Adequate information and details about the prices, goods and services offered	89.1%	84.9%	81.0%	86.8%	89.0%	90.0%
Vendors or manufacturers of goods or services guarantee (full refund or escrow)	74.3%	72.0%	74.7%	72.9%	73.6%	72.2%
Wide range of products and services	41.5%	52.2%	45.6%	46.0%	42.3%	43.5%
Good quality and value for the price	72.2%	83.5%	82.7%	88.0%	78.4%	77.6%
Instant response on your online payment transaction [b]	79.7%	89.9%	83.8%	66.2%	70.0%	70.9%
Payment option with cryptocurrency	85.3%	86.3%	77.4%	76.8%	79.9%	82.5%
Traditional offline payment option [a]	16.6%	16.9%	19.0%	30.2%	24.3%	23.7%
Online payment option [b]	63.2%	88.8%	77.9%	51.9%	50.7%	52.3%
Accessible, fast and easy payment transaction [b]	80.0%	88.9%	80.1%	70.7%	72.7%	74.4%
The web store page is easy to navigate	29.8%	46.0%	41.5%	51.2%	38.1%	38.7%
The popularity and positive feedback of the web store on the Internet [a]	75.0%	62.8%	72.3%	79.1%	80.5%	78.6%
The recommendation of the store by acquaintances or friends [a]	44.5%	46.1%	38.7%	54.9%	50.0%	52.0%
Discusses the rights and obligations of buyers and vendors information	54.5%	62.3%	60.0%	67.6%	59.2%	59.1%
The option of registering, or not, for browsing and purchases [b]	61.5%	70.2%	56.9%	43.0%	49.8%	52.3%
Protection of personal and purchase data [b]	91.5%	90.9%	87.6%	83.2%	87.0%	87.3%
Stable internet connection while shopping	63.2%	74.7%	66.1%	56.2%	56.4%	57.5%

5.2.2. University survey

For the university student survey, participants with greater knowledge in computer science, IT, or communications technology did not require a higher degree of trust when accessing illicit cryptomarkets compared to those who do not have expertise. However, when compared separately between the three different expertise areas, there were a few trust factors that respondents required a higher degree of trust for (detailed summary and comparison can be seen in *Table 5.2*). For those who identified as having greater expertise in computer science, IT, or communications technology, two trust factors were found to be more important in comparison to those without IT expertise: **(1) payment option with cryptocurrency,** and **(2) traditional offline payment options.** Participants with greater knowledge in medicine and the effects of drugs on humans, identified two trust factors as more important in comparison to their non-expertise counterparts: **(1) protection of personal and purchase data,** and **(2) the popularity and positive feedback of the web store on the internet.** Lastly, for those with greater knowledge in medicine, criminal law on illicit drug use, or other legal regulations, identified three trust factors as more important in comparison to their non-expertise counterparts: **(1) reliable delivery of goods, (2) instant response on your online payment transaction,** and **(3) vendor reliability.**

Even though there were no trust factors **that were found to be more important amongst those identifying as having expertise across the domains of IT, medicine, or law, there were several trust factors (n = 7) that those with expertise in all three areas considered less important in comparison to those with no expertise.** These can be seen in the cells that were not highlighted in the expertise columns in *Table 5.2.*

Table 5.1. University survey: Trust factors considered as important through comparing averages between expertise and non-expertise groups, across all scenarios. Identified important factors by the group are ones with higher percentage and are coloured. Note:[a] non-important trust factors identified by all expertise groups.

Trust Factors	Expertise Groups			Non-expertise Groups		
	IT	Medicine	Law	IT	Medicine	Law
Vendor contact and helpfulness	56%	76%	73%	73%	69%	69%
Vendor reliability	68%	83%	89%	93%	90%	88%
The popularity and positive feedback of the web store on the Internet	53%	69%	63%	66%	62%	64%
The recommendation of the store by acquaintances or friends [a]	65%	69%	63%	74%	73%	75%
The web store page is easy to navigate	54%	69%	63%	60%	56%	57%
Smooth internet connection while shopping	58%	72%	70%	60%	57%	56%
Protection of personal and purchase data	62%	86%	79%	84%	79%	81%
Discusses the rights and obligations of buyers and vendors information	47%	70%	66%	59%	54%	54%
The option of registering, or not, for browsing and purchases [a]	60%	49%	47%	65%	67%	69%
Instant response on your online payment transaction	54%	70%	79%	78%	74%	72%
Accessible, fast and easy payment transaction	68%	83%	87%	84%	81%	80%
Payment option with cryptocurrency	65%	30%	19%	39%	46%	50%
Traditional offline payment option	58%	34%	34%	47%	52%	54%
Online payment option	66%	85%	89%	72%	68%	66%
Vendors or manufacturers of goods or services guarantee (full refund or escrow)	52%	83%	86%	74%	67%	66%
Adequate information and details about the prices, goods and services offered	71%	86%	86%	84%	81%	80%
Wide range of products and services [a]	44%	36%	31%	45%	47%	49%
Good quality and value for the price [a]	66%	66%	68%	82%	82%	82%
Reliable delivery of goods	71%	86%	89%	92%	89%	88%
My real details should not even be known to the vendor [a]	60%	65%	60%	77%	76%	78%
My purchase information should be deleted immediately [a]	64%	69%	60%	79%	78%	81%
Opportunity to buy in a hidden and untraceable way [a]	64%	69%	73%	82%	80%	80%

5.3. Research Question Two Examination

Our second research question aimed to identify if individuals would prefer to purchase products illegally through online avenues in order to avoid legal repercussions relevant to purchases of drugs or firearms through legitimate means. We also questioned whether during this process, those with greater knowledge in technology, or having expertise in legal consequences around using or trafficking illicit products, are more likely to choose the darknet to purchase, in comparison to those who do not have this expertise. Results from both questions were analyzed for this hypothesis.

The comparison of responses between darknet users who have expertise in IT and communications technology or criminal law on illicit products and those who do not have expertise shows that **all darknet users, with or without expertise, are all more likely to purchase illegal products online**. For dark web users, the level of expertise in either IT or the legal field will not affect their decisions to make illegal purchases; the majority of the users all agree that purchasing online is more preferable than making purchases in-person[8].

In comparison, respondents from the university survey did give different responses depending on area of expertise. When comparing the responses between those with expertise in IT and communications technology, or criminal law on illicit drug use and other legal regulations to those without expertise, **university participants who have expertise are more likely to purchase online**. Answers from the two questions pertaining to the preference for purchasing were compared between the two groups, and results indicate that those with more expertise are more likely to choose to purchase online (54-85%). This is in contrast to the non-expertise counterparts, who were more likely to purchase in-person so they can see the product before purchasing (27–65%).

In the question where multiple options were given to allow participants to provide their preferences and reasoning for making illegal purchases, respondents gave mixed answers whether or not they had any form of expertise. However, within the subpopulation of respondents with no expertise, there seemed to be a slight preference towards purchasing in-person so as to see the goods, before they make the purchase. The only scenario in which this differed was in scenario five, in which both those with and without expertise seemed to favor purchasing online.

In addition to the breakdown of percentages between the two groups on why they would prefer in-person or online purchasing of illegal goods, five themes were identified from the open-ended question. As illustrated in *Figures 5.5* and *5.6*, those who have no expertise in either IT or law prefer to *meet in-person to protect personal privacy/details* (72%). In contrast, while this same theme did emerge amongst those who have expertise in either IT or law, this theme contained a smaller portion of responses (27%). The majority of those with expertise cited that they have a *mixed opinion depending on types of drugs, locations,*

[8] See *Appendix E* for a breakdown of results.

and prices (36%). Further, this mixed preference theme was not found within those answers from participants with no expertise, suggesting that those participants may not take these factors into consideration as much as those who have expertise.

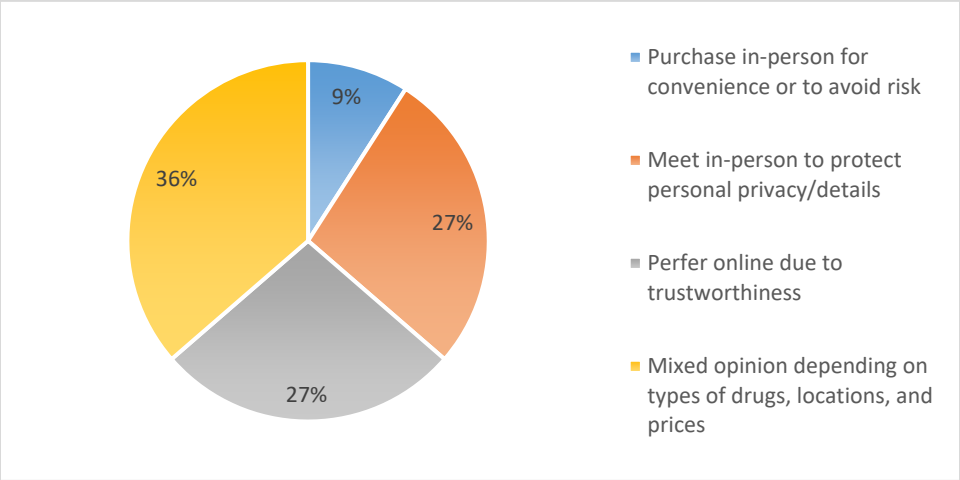

Figure 5.1. Themes of university survey participants with expertise who answered 'other' to why they would prefer in-person or online purchasing of products illegally.

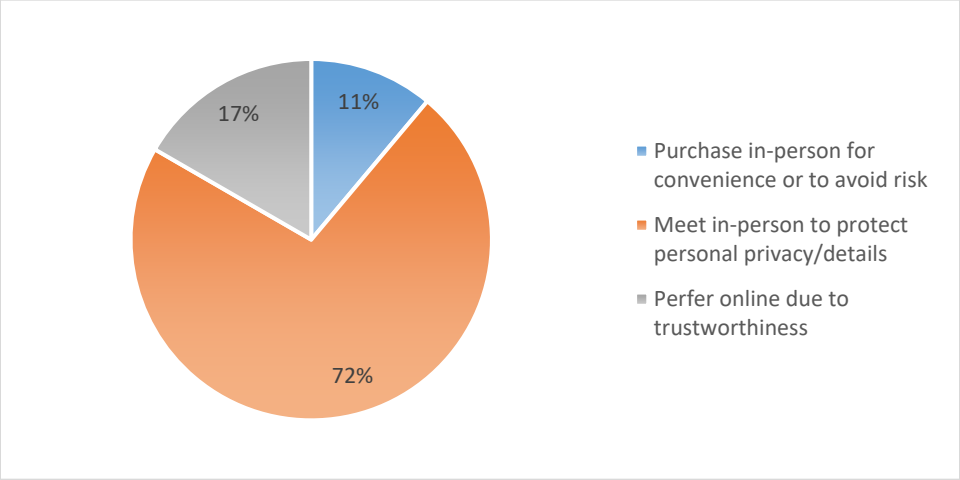

Figure 5.2. Themes of university survey participants without expertise who answered 'other' to why they would prefer in-person or online purchasing of products illegally.

5.4. Research Question Three (a) Examination

The first part of our third research question was closely related to the underlying pressure and level of urgency built within each scenario-based situation. More specifically, we wanted to understand whether buyers with more urgent need or compulsion are more likely to choose traditional methods to purchase illicit goods, and if they consider trust factors as less necessary when utilizing illicit darknet markets.

Ranking the scenarios in order of urgency, with the most urgent scenario listed following the legal scenario, and the least urgent scenario in the last column of the table,

comparisons can be made across the trust factors[9]. By ordering scenarios in this way, evaluations can be made regarding whether there are differences in the percentages of individuals who would prefer to choose traditional criminal methods as well as other trust factors in the scenarios. In comparing the trust factors across scenarios **for both the university as well as the darknet market survey respondents, there is not much difference in those responding that each trust factor is important**. It would be expected that the majority of the trust factors would be marked as less important in the more urgent scenario in comparison to the less urgent scenario, this was not found.

By comparing respondent answers for the questions about preference for a personal meeting, there is a clear difference in choosing to meet in person in comparison to online buying with the more urgent scenario for University students. While no difference was found when comparing answers for the same question across scenarios for darknet market users (see *Figure 5.7*), the least urgent scenario in the university study had a sharp increase in respondents choosing to purchase online instead of in person (see *Figure 5.8*). In fact, **darknet market users were more consistent in choosing to purchase the product online across all scenarios**, with only a slight increase in participants choosing to purchase in-person for scenario three.

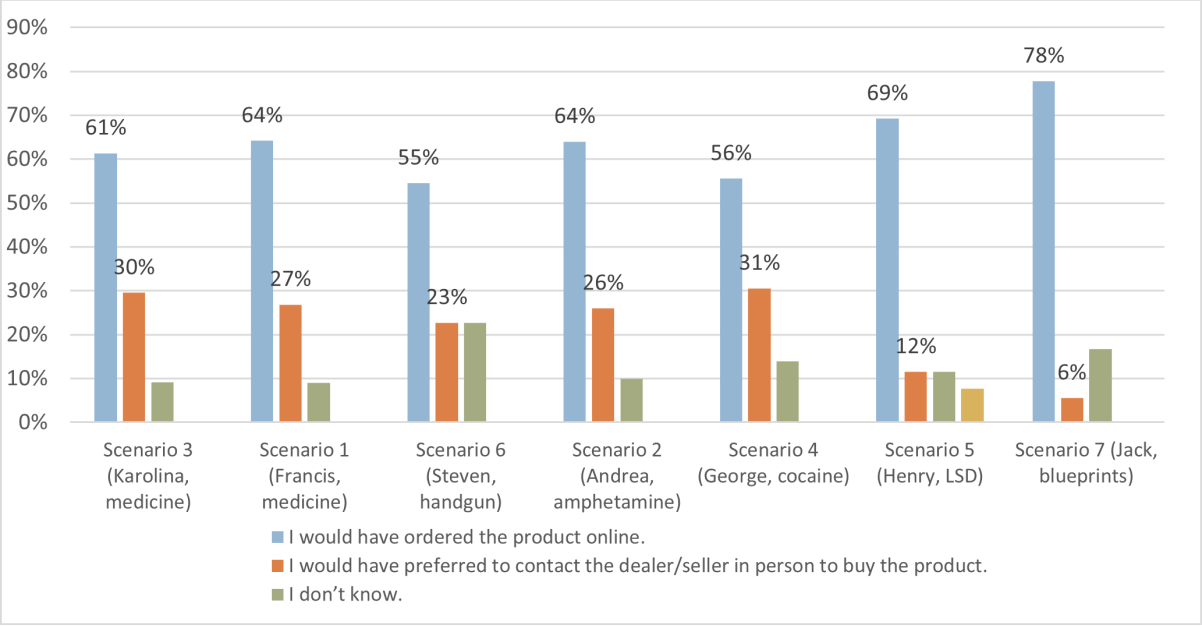

Figure 5.3. Darknet market survey results per scenario on where participants prefer to purchase a product illegally online or in-person. Ordered from most urgent to least urgent scenario.

[9] This table can be available upon request.

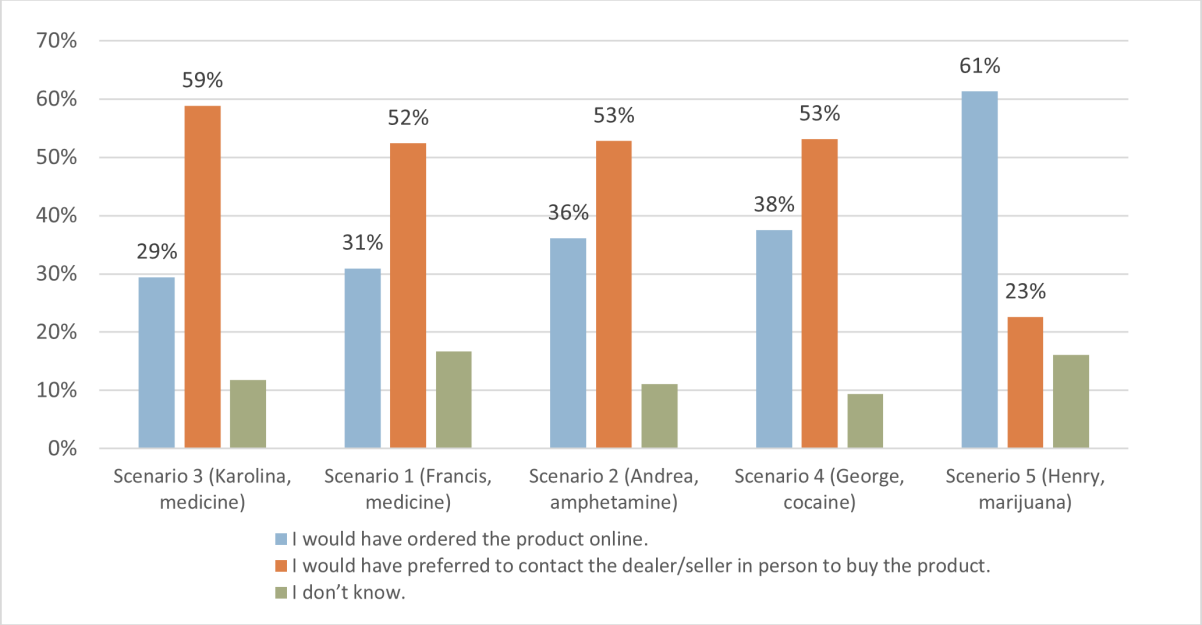

Figure 5.4. University survey results per scenario on where participants prefer to purchase a product illegally online or in-person. Ordered from most urgent to least urgent scenario.

In addition, when comparing answers for the question about why the respondent would rather purchase (online or in person), in-person meetings seem to be preferred in comparison to the least urgent scenario (scenario five) for university respondents. Across scenarios, university respondents answered '*It's important for me to be there in person when choosing the goods and be able to see what I buy*' most often (see *Figure 5.9*). Comparing both survey answers, the **university participants seem to be the only ones that factor in urgency when choosing to purchase online or in-person**. Lastly, an overall analysis of the themes found amongst the open-ended answers to why respondents choose in-person or online purchases, indicates that university students are more likely to purchase in person to '*protect their privacy and personal details*' (see *Figure 5.10*).

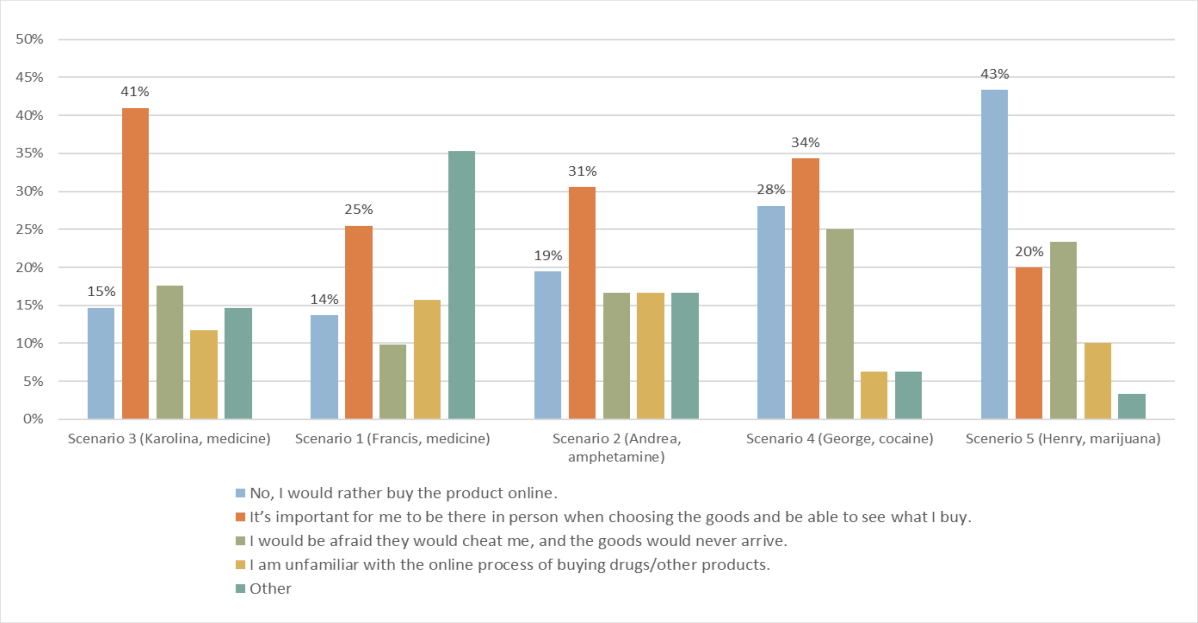

Figure 5.5. University survey results per scenario on why participants prefer to purchase a product illegally online or in-person. Ordered from most urgent to least urgent scenario.

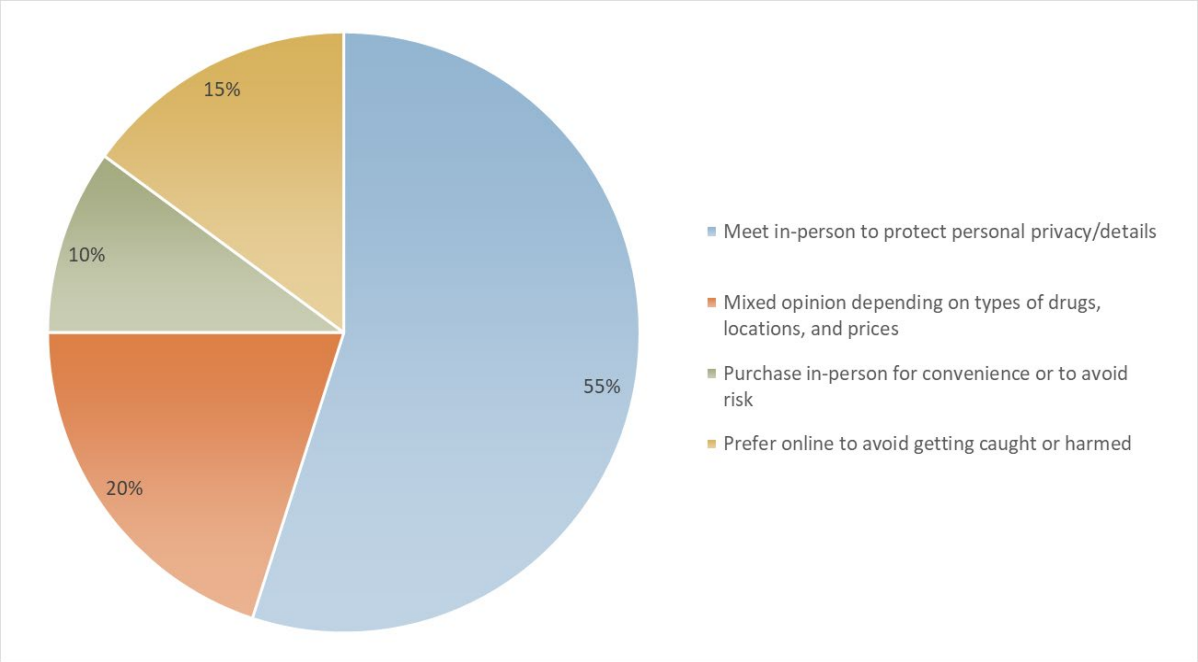

Figure 5.6. Themes of all university survey participants who answered 'other' to why they would prefer in-person or online purchasing of products illegally.

5.5. Research Question Three (b) Examination

In the case of the second part of our third research question, we were interested in whether individuals with greater knowledge in information technology (IT), the harmful

effects of illicit products, as well as legal consequences, require higher security to make purchases in illegal cryptomarkets.

A total of eight participants from the darknet market survey claimed to have expertise in IT, in medicine and the effects of drugs on humans, as well as having legal knowledge related to illegal products and trafficking. In their accounts of the events surrounding purchases of illicit products, confidence factors related to the trust category *secrecy and anonymity,* was the most important. In particular, all of the users agreed that '*opportunities to buy in a hidden and untraceable way*', having '*real details unknown to the vendors*', as well as having '*purchase information deleted immediately*' are extremely important when purchasing illicit products online. Participants also identified four other important trust factors to consider prior to initiating and completing a transaction in illegal cryptomarkets: (1) payment option with cryptocurrency; (2) the popularity and positive feedback of the web store on the internet; (3) the recommendation of the store by acquaintances or friends; and (4) discussions on the rights and obligations of buyers and vendors information. See *Table 5.3* for a breakdown of percentages of those with and without expertise who find these trust factors important.

Table 5.2. Difference between respondents with and without expertise on identifying specific trust factors as important.

Important Trust Factors	**With Expertise**	**Without Expertise**
Opportunities to buy in a hidden and untraceable	92.9%	83.3%
My real details unknown to the vendors	100%	66.7%
My purchase information deleted immediately	100%	50%
Payment option with cryptocurrency	100%	83.3%
The popularity and positive feedback of the web store on the internet	66.7%	60%
The recommendation of the store by acquaintances or friends	60.7%	60%
Discusses the rights and obligations of buyers and vendors information	81%	80%

Findings in the current study also revealed another five essential trust factors that are important to users with expertise in all of the three fields when making online purchases in general. In both situations where purchases can be made through either legal marketplaces or illegal cryptomarkets, all users (n = 8) agreed that factors such as '*vendor reliability*, *goods or service guarantee (e.g., full refund or escrow) provided by vendors or manufacturers*', '*instant response regarding online payment transaction*', '*options to have fast, easy and accessible payment transaction*', as well as '*protection of personal and purchase data*' are important (100%).

5.6. Research Question Four Examination

For the fourth research question, we wanted to identify whether or not, in situations where the first transaction in the illicit cryptomarket went smoothly, individuals are more likely to re-purchase from the same vendors in the future.

A **majority of the participants in both surveys agreed that successful transactions would increase their willingness to repurchase** (see *Figure 5.11* and *Figure 5.12*). This holds true over the majority of scenarios posed in the surveys. The one exception to this finding is in the university study, in which only 36% of respondents agreed they would repurchase, whereas a slightly higher percentage of 39% claimed they would not repurchase.

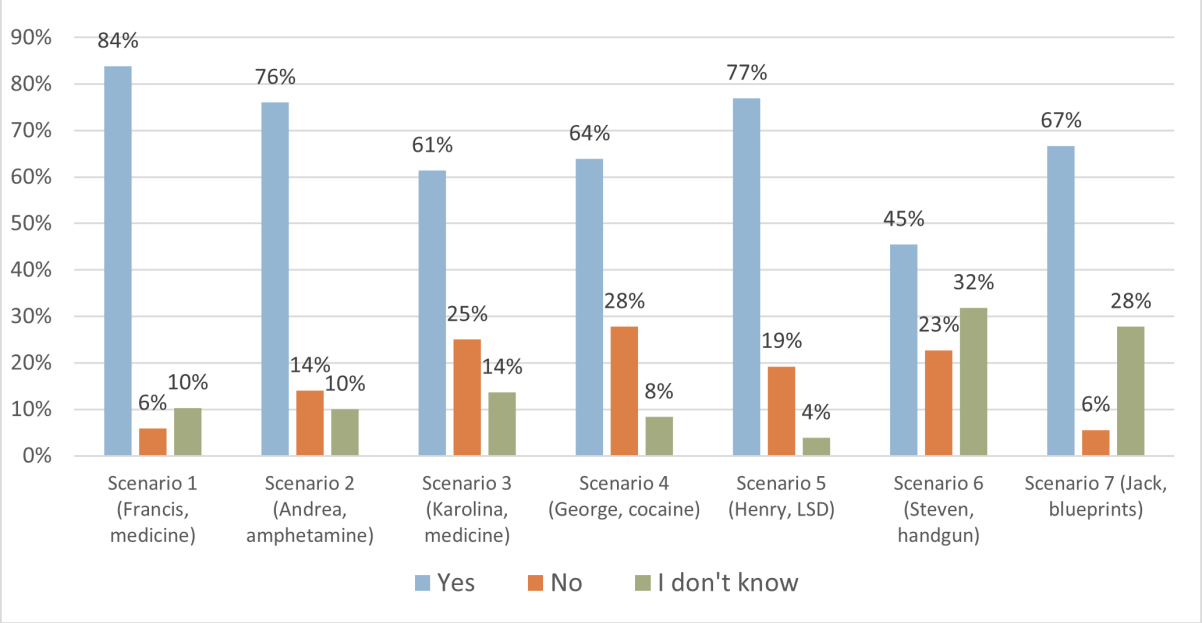

Figure 5.7. Darknet market survey responses on whether or not they would repurchase from the same vendor following a successful transaction.

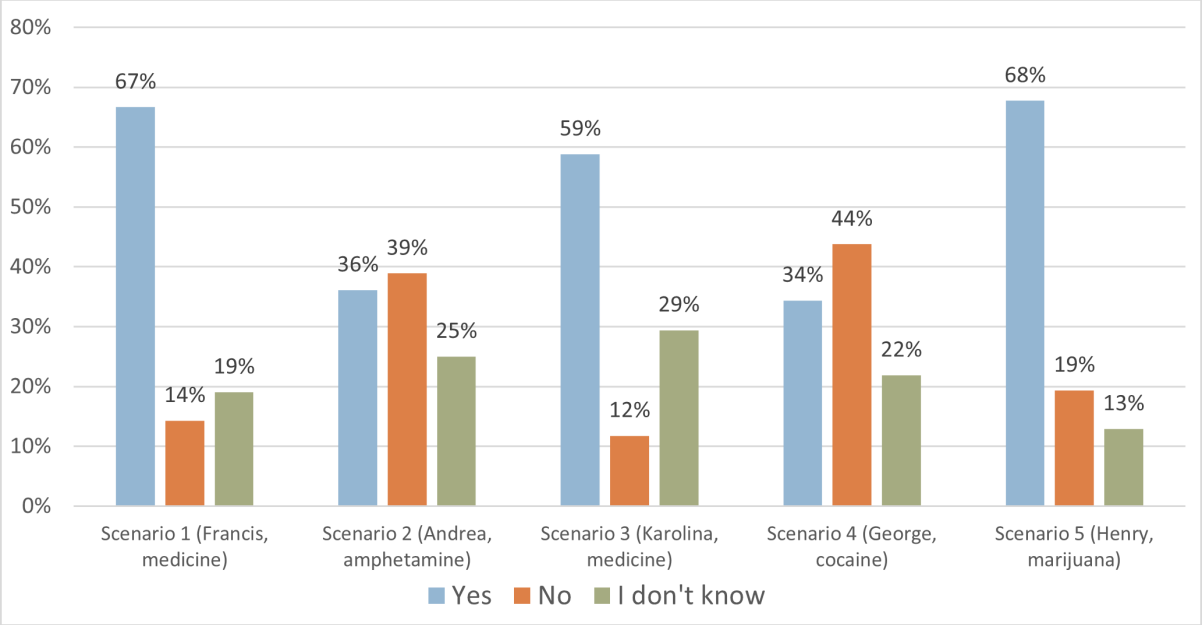

Figure 5.8. University survey responses on whether or not they would repurchase from the same vendor following a successful transaction.

5.7. Research Question Five Examination

For our last research question, we focused on the set of trust categories representing the anonymous and covert conditions relevant to online purchases. We wanted to identify whether individuals consider trust factors focusing on anonymity and secrecy as more important in conditions where illicit products are purchased.

Results indicate that **respondents in both the darknet and the university student survey regarded the trust factors of secrecy and anonymity as being more important in the illegal scenarios, in comparison to the legal scenario**. *Figures 5.13* and *5.14* provide the percentages of participants in each scenario, stating that these three trust factors are either *absolutely required* or *very important* more often than when answering the same questions in the legal scenario.

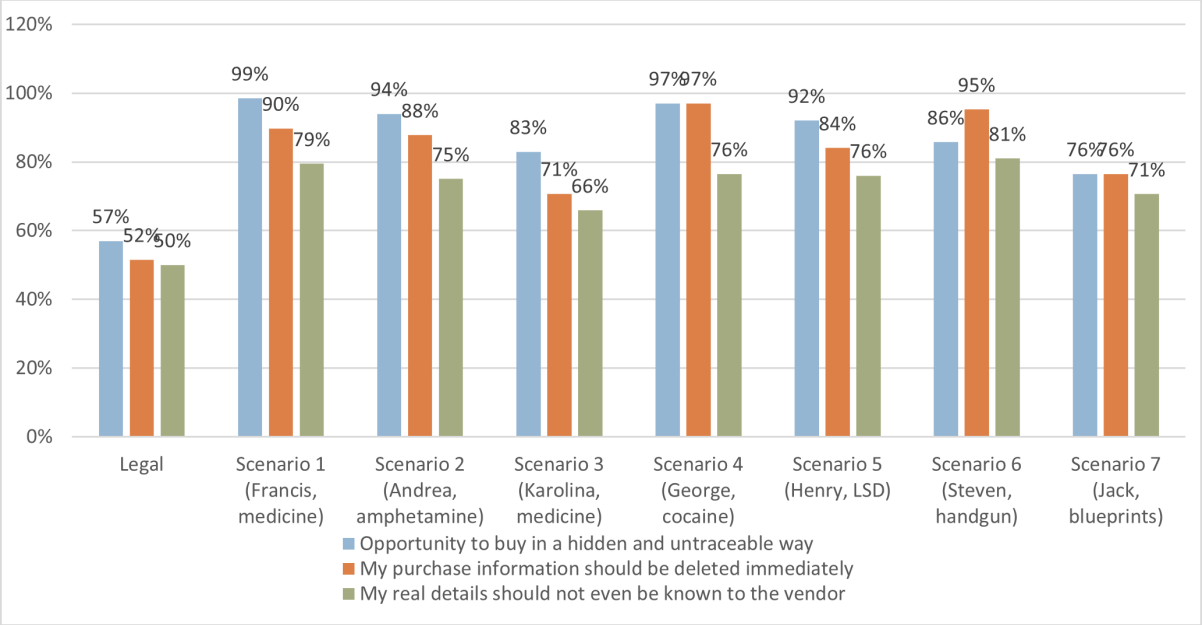

Figure 5.9. Percentages of Darknet market survey participants stating that the three secrecy and anonymity trust factors are either absolutely required or very important in their decision to trust the online vendor.

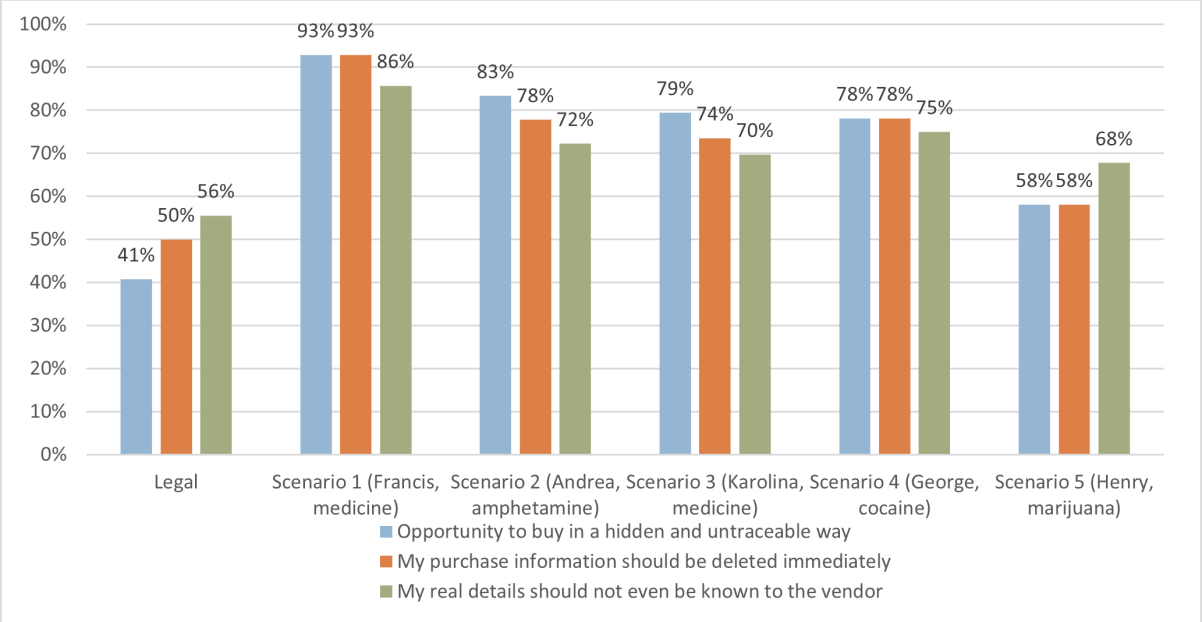

Figure 5.10. Percentages of university survey participants stating that the three secrecy and anonymity trust factors are either absolutely required or very important in their decision to trust the online vendor.

Chapter 6. Discussion

With the ever-evolving landscape of cyber related crimes, the market for purchasing illicit firearms and drugs is becoming more prevalent within darknet markets. Individuals are able to purchase illicit goods within these markets, evading any in-person deals and related potential risks (Becker, 1974; Cornish & Clarke, 1986; Cohen & Felson, 1979; Thibaut & Kelley, 1959). This shift online may be due to darknet markets offering a level of anonymity not usually offered by those purchasing illicit goods through traditional online methods (Linder, 2019). However, in order for these markets to be successful, a level of trust must be established between buyers and vendors of these markets. Trust is an important aspect of any relationship, and especially so within the entrepreneurial world; not only does trust help to reduce any potential risks for both buyer and vendor, it also helps build relationships between the two parties (Welter, 2012). Not unlike licit markets, trust within these darknet markets is necessary for vendors and buyers, who may both be wary of law enforcement (Tzanetakis et al., 2016). Therefore, trust is an invaluable tool that aids in successful transactions between two parties; for this reason, it is essential that the specific trust factors which are most important within these illicit marketplaces be identified to aid law enforcement in taking down these markets. The purpose of the current study was to understand the basis for which trust is established within both firearms and drug darknet markets. This was accomplished by answering five research questions, each touching on differing aspects of participant expertise, and the trust factors necessary for a transaction. By surveying possible darknet market users, as well as university students, we were able to identify which trust factors are most important for both experienced and non-experienced users of these markets, thereby adding to what we currently understand about how trust is established within these communities. The results of this study may aid law enforcement in future investigations of these marketplaces, and those who use them.

Results from the two surveys indicate that darknet market and university respondents differ in how they respond to the scenario-based questions. For instance, responses from the darknet market survey revealed that those with expertise in the areas of IT, the effects of illicit drugs, or the legal consequences of trafficking or using illicit products, consider specific trust factors to be important in comparison to those without expertise. Darknet market respondents identified five factors that were more important when respondents had expertise in one of the three areas: **(1) instant response on your online payment transaction; (2) online payment option; (3) accessible, fast and easy payment transaction; (4) the option of registering, or not, for browsing and purchases;** and **(5) protection of personal and purchase data.** However, in the university study there were no trust factors across all areas of expertise that were found to be more important in comparison to those without expertise. We can surmise from this that while respondents of the university survey do not differ much in terms of having expertise in a given field and expecting more trust factors to be met, those respondents of the darknet market survey indeed differ when one has expertise in a field or not. The difference between responses may be that university students are less familiar with shopping on these darknet markets,

and so there is an equal emphasis for trust to be required among respondents, regardless of expertise. However, when respondents are more familiar with shopping in these darknet markets (as in darknet market respondents), having expertise in a certain field will translate to requiring more measures of trust to be met.

Another finding from this study was that darknet market respondents with expertise in either IT or legal repercussions are no different than those without such knowledge when it comes to preferring to purchase online or in-person; both subgroups are equally likely to choose the dark web to purchase these products even when legal options for purchasing are available. However, there was a difference between those with expertise in these two areas, and those without within the university population, with 36% of respondents preferring to meet in person to '*protect personal details or avoid risk*'. In contrast, 83% of those in the university study without expertise preferred to meet in person for these same reasons. This could be because those who are less familiar with IT or legal repercussions do not understand the safety of these illicit darknet markets, and so will favour purchasing in-person. These results then highlight the differences between individuals who may have more experience with darknet markets, and those without (university students). **Those who are more familiar with these markets are more likely to purchase online, whereas those who are less familiar are only more likely to purchase online if they have expertise in a given field.**

What also differed between the darknet market and university student surveys were their responses to questions based on scenario urgency. We found that trust factors remained consistently important regardless of level of scenario urgency in both surveys, however there was a slight favour for those university respondents in the urgent scenarios to prefer to meet in person. Of university respondents, 65% preferred to meet in-person to '*protect personal details or for convenience and to avoid risk*'. These results indicate that **darknet market and university students find trust to be equally important regardless of urgency**, while **university respondents may be more willing to purchase in person in the most urgent scenario**.

What was found to be consistent between respondents in both surveys were responses to repurchasing a product, as well as the importance of secrecy and anonymity. In both surveys, we found that **once an individual successfully makes a transaction within these darknet markets, there is a high probability that they will purchase from that vendor again in the future**. Therefore, it's possible that a large portion of the buyers within these markets are repeat buyers, and that trust may be built upon prior success with transactions. This further supports previous findings that past transactions are what aids in building trust for buyers within these markets (Norbatus et al., 2020a; Linder, 2019; Norbatus et al., 2020b). Additionally, respondents in both the darknet market survey, as well as the university survey found **trust factors related to secrecy and anonymity to be more important when making illicit online purchases**. In comparison to the legal scenario, respondents from both surveys had identified that the three trust factors '*opportunity to buy in a hidden and untraceable way*', '*my purchase information should be deleted immediately*', and '*my real details should not even be known to the vendor*' had more

responses of *absolutely required* or *very important* than the legal scenario. This addresses the need for buyers to have complete confidentiality through means of anonymous paying methods as well as to have their account of shipping details removed when making illicit purchases within these markets. If these concerns are not met with a particular market or vendor, there is a higher probability that buyers will go elsewhere, and the market or vendor will not last. Therefore, these specific factors may aid in identifying who may be key players within these illicit spaces.

Lastly, while this study aimed to answer specific questions related to trust within these markets, one of the final goals was the creation of a trust matrix which may be used to aid law enforcement in their investigations of these markets. The resulting trust matrix depicts percentages of respondents from each survey that consider each trust factor to be important, and can be viewed in *Appendix F*. Overall, 12 factors were found to be important across all scenarios and for respondents from both surveys (with a cutoff above 65% considered important). Specific to the university students, who may be less familiar with purchasing illicit products within darknet markets, the trust factors '*the recommendation of the store by acquaintances or friends*' and '*online payment method*' were found to be important. In contrast, darknet market users specifically identified '*payment option with cryptocurrency*' and '*the popularity and positive feedback of the webstore on the internet*' as important factors.

These findings highlight the variances between these two populations, in that those who may be less familiar with darknet markets (university students) will tend to rely more on traditional means when purchasing and determining trustworthy vendors or products within these markets. Those who are more familiar (darknet market users) are more likely to rely on more technologically driven factors. For instance, instead of relying on known contacts such as friends or acquaintances to provide feedback about a vendor (as is the case with university students) respondents in the darknet market survey rely more on positive feedback from strangers who are leaving their feedback online. These may not be as trusted as sources as friends or family, but they offer a convenient tool for feedback that can only be accessed online, and which further creates a sense of anonymity when using these darknet markets.

6.1. Summary

The majority of research questions set forth in this study provided inconsistent results between the university and darknet market survey respondents, with just two of the research questions (four and five) having consistent results between both populations. It is more likely that darknet market users are more familiar with technology, not only because more respondents had identified that they had expertise in IT (n=33), but also because more respondents (n=62) from the darknet market survey identified that they use browsers that conceal their identity. These factors may then make up for some of the discrepancies between surveys. If respondents in the darknet market survey are already more familiar with technology, and purchasing online, there may not be large differences between those who have expertise and those who may not have expertise. In comparison,

the difference between having expertise or not in the university survey did make a difference, and this could be because this population as a whole is less familiar with the use of darknet markets. Therefore, a difference between having expertise and not within the darknet market survey population, may be completely different than the difference between having expertise or not within the university survey population.

Findings from this study may support previous assertions that vendors who have built up trust among buyers, will continue to use their vendor name across markets (Norbatus et al., 2020b), since a majority of respondents in our surveys had claimed they would repurchase following a successful transaction. It would follow then, that vendors will use this to their benefit and choose to keep their name across markets so as to keep the trust of the customer base they have already built up. These results also suggest that building trust within these communities differs between those who are familiar with such transactions and those who may not be as familiar. It is assumed that the respondents from the darknet market survey had more experience purchasing illicit goods online in comparison to those university respondents, even though they were recruited through Reddit. This was evident as there were differences in how respondents in both surveys responded to scenario-based questions. Thus, it could be suggested that those with a higher degree of knowledge in IT or the legal issues surrounding purchasing or selling illicit goods, are more likely to become buyers in these darknet markets, in comparison to those who may not have this type of knowledge. This also suggests that those who use these markets may be younger in age than the average person who would sell or purchase these goods in-person, and that as technology continues to be relied upon and more generations grow up with it, these markets will also continue to grow.

Chapter 7. Conclusion

Trust within darknet markets is essential as it enables vendors to make sales, and aids buyers with choosing the safest vendor. The aim of this study was to establish the decision-making factors involved with purchasing illicit items from darknet markets, to better understand which trust factors are most important. This study differed from previous studies in that it surveyed individuals about their views on trust in online drug and firearm darknet markets. By doing so, we were able to analyze different aspects of trust, such as differences between buyer experience in fields of expertise, and assessing their responses to specific scenarios.

Future researchers may want to tread lightly on extrapolating these results, as there were a few limitations to the study. Unfortunately, due to restrictions with advertising the survey within these darknet market forums, we were unable to access vendors to participate in our survey. Even so, the population of individuals targeted with the survey advertisement over specific subreddits allowed for access to a population who may be users of these markets. Responses from these participants validate this reasoning, as the majority of respondents identified as being darknet users within the survey. While we were able to assess this similar population in addition to the university population, there

were still few completed surveys overall. Also, those who had participated in the survey were unlikely to complete the survey until the end, with only 17% of respondents from the darknet market survey, and 56% of respondents from the university survey having completed the final scenario question. Even so, these results are an important step in understanding which trust factors are most important for firearm and drug darknet market users.

Overall, recommendations for law enforcement are to monitor these markets to identify those that may have staying power based on the secrecy and anonymity factors employed. Additionally, specific vendors may want to be monitored to assess those that may be particularly popular, in terms of number of positive reviews, which may suggest that these specific vendors are active within other cryptomarkets. Knowing that vendors are likely to use the same name across various darknet marketplaces, and to inherit on the trust they have built from previous transactions, it would therefore be easier for law enforcement to identify and flag identical and potentially larger vendors active in these marketplaces. Further, law enforcement may want to consider working with cryptocurrency exchange platforms to aid in investigating, and potentially connecting, anonymous crypto wallets with individuals engaging in illicit transactions. For example, larger exchange platforms such as Coinbase, commonly used by individuals engaging in cryptocurrency exchange, require their users to provide information to verify their identities (Coinbase, 2022). Lastly, by understanding the backgrounds of those individuals most responsible for using these darknet markets, regarding age and technological skill, a better understanding of the profiles of these individuals may aid law enforcement in developing a profile of common users.

References

Becker, G.S. (1974). *The economic approach to human behavior.* Chicago, IL: University of Chicago Press.

Botsman, R. (2017, December 21). How Darknet Sellers Build Trust. *Nautilus* (55).

Bradley, C. (2019). *On the resilience of the Dark Net Market ecosystem to law enforcement intervention* (ProQuest Dissertations Publishing).

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F., and Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, *264*, 7–14.

Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., and Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence, 173*, 159–162.

Cohen, L.E., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Coinbase. (n.d.). Coinbase User Agreement. Retrieved May 6, 2022.

Cornish, D.B., and Clarke, R.V. (1986). *The reasoning criminal: Rational choice perspectives on offending.* New York: Springer-Verlag.

Copeland, C., Wallin, M., and Holt, T.J. (2020). Assessing the Practices and Products of Darkweb Firearm Vendors. *Deviant Behavior*, *41*(8), 949–968.

Décary-Hétu, D., and Giommoni, L. (2016). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75.

Dingledine, R. (2002, September 20). "Pre-alpha: run an onion proxy now!". or-dev@freehaven.net (Mailing list). Archived from the original on 26 July 2011. Retrieved 17 July 2008.

Frank, R. (2020). The Dark Crawler.

Kiss, T., Parti, K., and Prazsák, G. (2019). Cyberdeviancia. *Dialóg Campus*, 55–133.

Lane, B., Lacey, D., Stanton, N., Matthews, A., and Salmon, P. (2018). The Dark Side Of The Net: Event Analysis Of Systemic Teamwork (East) Applied To Illicit Trading On A Darknet Market. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62*(1), 282–286.

Linder, C. (2019). Chapter 8 The Entrepreneurial Criminal: How Trust Coordinates Illicit Drug Cryptomarkets. In B.S. Sergi & C.C. Scanlon (Eds.), *Entrepreneurship and Development in the 21st Century* (pp. 171–189). Emerald Publishing Limited.

Morselli, C., Giguère, C., and Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks, 29*(1), 143-153.

Norbutas, L., Ruiter, S., and Corten, R. (2020a). Believe it when you see it: Dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs. *Social Networks*, *63*, 150–161.

Norbutas, L., Ruiter, S., and Corten, R. (2020b). Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets. *International Journal of Drug Policy*, *76*, 102635.

Paoli, G.P., Aldridge, J., Ryan, N., and Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.* RAND Corporation.

Tibor, K., Ákos, S., and László, D. (2020). A vásárlói e-bizalom szerepe az illegális szerek online kereskedelmében (Kézirat).

Thibaut, J.W., and Kelley, H.H. (1959). *The social psychology of groups.* New York: John Wiley & Sons.

Tzanetakis, M., Kamphausen, G., Werse, B., and von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, *35*, 58–68.

UNODC. (2020a). *World Drug Report. Book 4. Cross-cutting issues: Evolving trends and new challenges*.

UNODC. (2020b). *Transnational organized crime facilitated through technology: The Phantom Secure case.*

Welter, F. (2012). All you need is trust? A critical review of the trust and entrepreneurship literature. *International Small Business Journal: Researching Entrepreneurship*, *30*(3), 193–212.

Appendix A. Trust Categories and Confidence Factors[10], along with additional scenario-based questions

Trust Categories	Confidence Factors
Individual and community	1. Vendor contact and helpfulness 2. Vendor reliability 3. The popularity and positive feedback of the web store on the internet 4. The recommendation of the store by acquaintances or friends
Technology and network	5. The web store page is easy to navigate 6. Smooth internet connection while shopping
Data protection and privacy and legal information	7. Protection of personal and purchase data 8. Discusses the rights and obligations of buyers and vendors information 9. The option of registering, or not, for browsing and purchases
Payment transaction	10. Instant response on your online payment transaction 11. Accessible, fast and easy payment transaction 12. Traditional offline payment option 13. Payment option with cryptocurrency 14. Online payment option
Products and services	15. Wide range of products and services 16. Vendor's or manufacturers of goods or services guarantee (full refund or escrow) 17. Adequate information about the prices, goods and services offered 18. Good quality and value for the price
Transportation services	19. Reliable delivery of goods intact
Secrecy and anonymity	20. Opportunity to buy in a hidden and untraceable way 21. My purchase information should be deleted immediately 22. My real details should not even be known to the vendor
Additional scenario-based questions	**a.** ...would you recommend the website to someone else? * **b.** ...would you buy from the vendor if you were in a similar situation? **c.** ...the option of buying the medicine online or in person, where would you rather buy it from? **d.** ...in-person instead of online? Why? You can suggest other options!

**Note: Questions a.–d. differed in language used at beginning of question depending on scenario.*

[10] The trust categories and confidence factors were retrieved from the manuscript published by Tibor et al. (2020). See Tibor, K., Ákos, S., & László, D. (2020). A vásárlói e-bizalom szerepe az illegális szerek online kereskedelmében (Kézirat).

Appendix B. Scenario Situations for Darknet Market Survey

Scenario	Situation
1. (Francis, medicine)	Francis is a middle-aged man who lives with his mother, Elizabeth, in low-cost housing. Elisabeth underwent several joint surgeries due to an accident. She feels unbearable pain from her knee and hip joints. Elizabeth cannot sit, stand, or lie down without suffering. The recovery period is estimated to take a few months, which seems to be an eternity for both Francis and Elizabeth. Francis begs the doctor for a stronger painkiller in vain. The doctor can only prescribe medications that are no longer effective for Elizabeth. Francis' cousin had some tablets with high codeine content. The codeine was given to Elizabeth and she was in better shape thanks to the drug. The codeine lasted her a few days, but once it ran out, she was in pain again. Francis decided to help with his mother's pain by visiting his cousin and asking where to get codeine. Francis was told that it was an order from a dark net market, and that it wasn't legally available. He decided to order enough to last for a few months, until the recovery period was over. There are several vendors selling drugs that contain codeine, similar to the one he got from his cousin. Francis currently has to investigate which sites would be the more reliable for purchase.
2. (Andrea, amphetamine)	Andrea wanted to be a doctor all her life, so after graduation, she entered the medical school she applied for without scholarships or other funding. Since Andrea has no siblings, her parents and grandparents all saved their fortunes to pay for Andrea's schooling. She did not abuse the trust of her family, she didn't fail any classes and reached the last semester. In the last semester, she was overloaded from several events and failed two final exams. Andrea knows that if she does not pass those classes, she wouldn't be able to take the qualifying exam and would have to repeat the year. Her family could not pay for another year. Thankfully, the professor allowed a retest in each subject out of consideration of the major events that occurred in Andrea's life. Both the exams were in a week because the graduation deadline was at the end of the week. Andrea only has 6 days left to prepare. She started studying hard but doesn't feel like she could finish studying because she kept falling asleep. Coffee and other caffeinated products were not effective anymore. Her friends suggested getting some amphetamine-containing tablets that can improve performance for a short period of time so she can study more and pass her exams. Andrea decided to get the drug

Scenario	Situation
	at the suggestion of her friends and plans to use the internet to get them. To order drugs, she visited multiple markets and is wondering which one would be most reliable for her purchase.
3. (Karolina, medicine)	Karolina is a mother in her 30s. She is raising three children with her husband in a small town. They found out two months ago that one of her children suffers from a rare disease that results in complete physical and mental degradation over the course of a few years. The disease can be cured with a very expensive drug they buy from abroad. They do not have much time, the young boy's condition will be irreversible in a few months if there is no medication available. Karolina is raising money, but the money is only half gathered. One day, one of her acquaintances suggested that she shouldn't wait, and to go online to look for similar medicine online. He said that he researched a site selling illegal drugs where he found medicine for his child, at a much cheaper cost compared to the original. Karolina should be able to afford it more easily. She knows that if you collect the donations to buy the drug legally, it will take longer. The longer it takes, the more her child's mental and physical condition deteriorates. Karoline felt she had to get the drug at any cost from one of the dark net markets. She isn't sure which would be the more reliable.
4. (George, cocaine)	George is a 25-year-old man who is a manager at a large international company. He does amazing work and receives a high pay so he can live a luxurious lifestyle. Company expectations have been growing higher and George is no longer able to withstand the stress, so to increase performance, he consumes cocaine. The drug is delivered by a drug dealer every time George calls him. One day, the drug dealer was arrested by the police. The arrest happened exactly when George's boss promised that if the quarterly performance doubles, George can have a more relaxed work schedule with the same pay. George needs a lot of cocaine now, having a month left to meet the challenge and change his life. He decided to go online and order the drug himself. George searched for a site to buy cocaine, but still doesn't know which would be the most reliable.
5. (Henry, LSD)	Henry grew up as close friends with his cousin, Andrew. As adults, Henry went to university to study computer science while Andrew went into welding. When Henry was laid off and couldn't pay the rent of his apartment, Andrew offered a room for him to use. A few weeks later, Henry was able to get a new job and rent his own

Scenario	Situation
	apartment. Henry was grateful for Andrew's kindness. Some time later, Andrew asked for a favor. He wanted buy LSD but felt that it had been too risky to go out in person lately. Andrew heard that it was possible to buy LSD online, but that there were complicated steps. Andrew went to Henry to ask if he could help buy them, and that he would pay Henry back. Henry agrees to order LSD online for his cousin, since he had more knowledge about computers and more experience in navigating the web. He found a number of different sites, but it's his first-time buying drugs online, so he doesn't know where to order from that would be most reliable.
6. (Steven, handgun)	Steven just moved to a new area and lives alone. Recently, he saw a mugging close by his home and is worried that he could be next. He doesn't feel safe. Steven is nervous every time he leaves home and sometimes, even within his home. As days pass, Steven sees more violence and fears that he will be attacked soon. He doesn't have a firearm license, but considers getting one later on. Steven decides to buy a handgun and ammo online for self defense. Since it's Steven's first time buying a handgun online, he isn't sure what would be the most reliable site or vendor to buy from.
7. (Jack, blueprints)	Jack was sitting at home when news came up about how the government intends to ban certain firearms and introduce laws around 3D printed guns. Jack and his friends go out target shooting every month with all sorts of rifles and handguns. They all have a good time and go home happy at the end of their monthly meeting. Jack believes having a 3D printed gun would be interesting to try. He already has a 3D printer and can print a few guns to use at target practice with his friends. Jack decides to go online to buy the blueprints for the gun, and has found something that seems reputable, but since it's his first time buying a 3D gun blueprint, he is a bit worried.

Appendix C. Scenario Situations for University Survey

Scenario	Situation
1. (Francis, medicine)	Francis is a middle-aged man who lives with his mother, Elizabeth, in low-cost housing. Elisabeth underwent several joint surgeries due to an accident. She feels unbearable pain from her knee and hip joints. Elizabeth cannot sit, stand, or lie down without suffering. The recovery period is estimated to take a few months, which seems to be an eternity for both Francis and Elizabeth. Francis begs the doctor for a stronger painkiller in vain. The doctor can only prescribe medications that are no longer effective for Elizabeth. Francis' cousin had some tablets with high codeine content. The codeine was given to Elizabeth and she was in better shape thanks to the drug. The codeine lasted her a few days, but once it ran out, she was in pain again. Francis decided to help with his mother's pain by visiting his cousin and asking where to get codeine. Francis was told that it was an order from a dark net market, and that it wasn't legally available. He decided to order enough to last for a few months, until the recovery period was over. There are several vendors selling drugs that contain codeine, similar to the one he got from his cousin. Francis currently has to investigate which sites would be the more reliable for purchase.
2. (Andrea, amphetamine)	Andrea wanted to be a doctor all her life, so after graduation, she entered the medical school she applied for without scholarships or other funding. Since Andrea has no siblings, her parents and grandparents all saved their fortunes to pay for Andrea's schooling. She did not abuse the trust of her family, she didn't fail any classes and reached the last semester. In the last semester, she was overloaded from several events and failed two final exams. Andrea knows that if she does not pass those classes, she wouldn't be able to take the qualifying exam and would have to repeat the year. Her family could not pay for another year. Thankfully, the professor allowed a retest in each subject out of consideration of the major events that occurred in Andrea's life. Both the exams were in a week because the graduation deadline was at the end of the week. Andrea only has 6 days left to prepare. She started studying hard but doesn't feel like she could finish studying because she kept falling asleep. Coffee and other

Scenario	Situation
	caffeinated products were not effective anymore. Her friends suggested getting some amphetamine-containing tablets that can improve performance for a short period of time so she can study more and pass her exams. Andrea decided to get the drug at the suggestion of her friends and plans to use the internet to get them. To order drugs, she visited multiple markets and is wondering which one would be most reliable for her purchase.
3. (Karolina, medicine)	Karolina is a mother in her 30s. She is raising three children with her husband in a small town. They found out two months ago that one of her children suffers from a rare disease that results in complete physical and mental degradation over the course of a few years. The disease can be cured with a very expensive drug they buy from abroad. They do not have much time, the young boy's condition will be irreversible in a few months if there is no medication available. Karolina is raising money, but the money is only half gathered. One day, one of her acquaintances suggested that she shouldn't wait, and to go online to look for similar medicine online. He said that he researched a site selling illegal drugs where he found medicine for his child, at a much cheaper cost compared to the original. Karolina should be able to afford it more easily. She knows that if you collect the donations to buy the drug legally, it will take longer. The longer it takes, the more her child's mental and physical condition deteriorates. Karoline felt she had to get the drug at any cost from one of the dark net markets. She isn't sure which would be the more reliable.
4. (George, cocaine)	George is a 25-year-old man who is a manager at a large international company. He does amazing work and receives a high pay so he can live a luxurious lifestyle. Company expectations have been growing higher and George is no longer able to withstand the stress, so to increase performance, he consumes cocaine. The drug is delivered by a drug dealer every time George calls him. One day, the drug dealer was arrested by the police. The arrest happened exactly when George's boss promised that if the quarterly performance doubles, George can have a more relaxed work schedule with the same pay. George needs a lot of cocaine now, having a month left to meet the challenge and change his

Scenario	Situation
	life. He decided to go online and order the drug himself. George searched for a site to buy cocaine, but still doesn't know which would be the most reliable.
5. (Henry, marijuana)	Henry meets with his foreign friends in Toronto every other month, where they have fun and use marijuana wrapped in cigarette paper. Everyone is in a very pleasant mood at the end of each meeting, so Henry is really looking forward to the next meeting. However, so far, his friends have provided the marijuana every time. Now it's his turn. Henry decided to order weed online, he searched the internet and found a website selling marijuana. It's his first time buying drugs online, so he doesn't know where to order from that would be most reliable.

Appendix D. Breakdown of Research Questions

Breakdown of research questions by subgroups, trust factors, and whether or not results supported each.

Research Question	Subgroup	Trust Factors	Result
One	Darknet	All Factors	Supported
	University	All Factors	Not supported
Two	Darknet	Qs: c, d	Not supported
	University	Qs: c, d	Supported
Three (a)	Darknet	All Factors; Qs: c, d	Not supported
	University	All Factors; Qs: c, d	Partially supported
Three (b)	Darknet	All Factors	Not supported
	University	All Factors	Not supported
Four	Darknet	Q: b	Supported
	University	Q: b	Supported
Five	Darknet	Factors: 20, 21, 22	Supported
	University	Factors: 20, 21, 22	Supported

Appendix E. Figures Depicting Results for Research Question Two

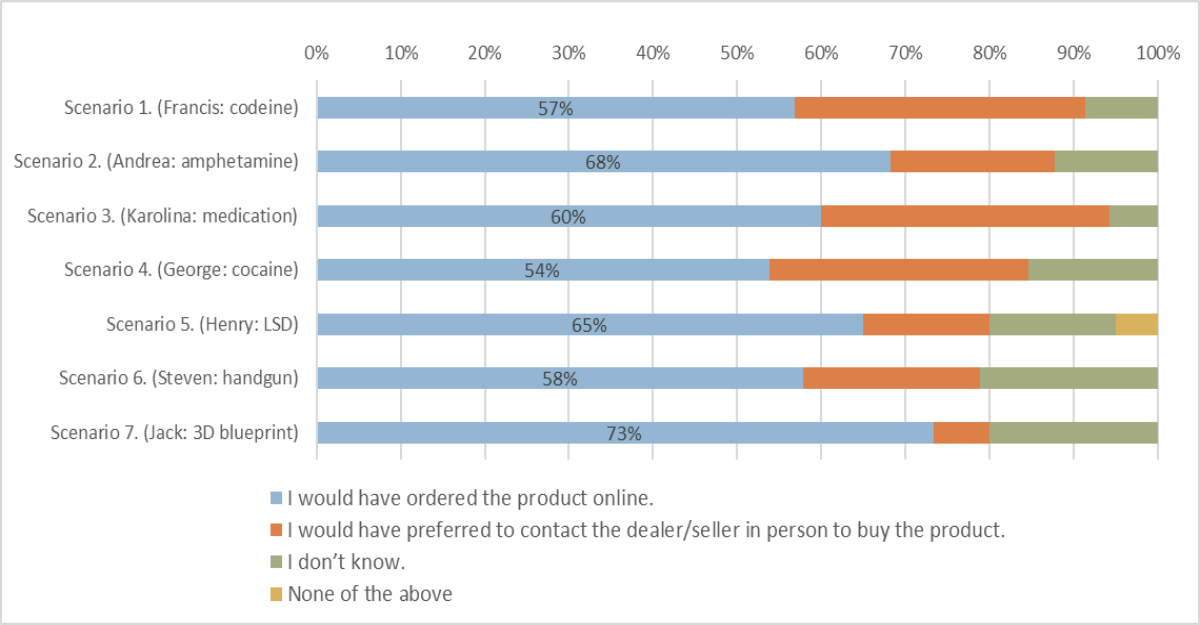

Figure E.1. Darknet survey respondents with either IT or law expertise, on where they would rather purchase products from illegally.

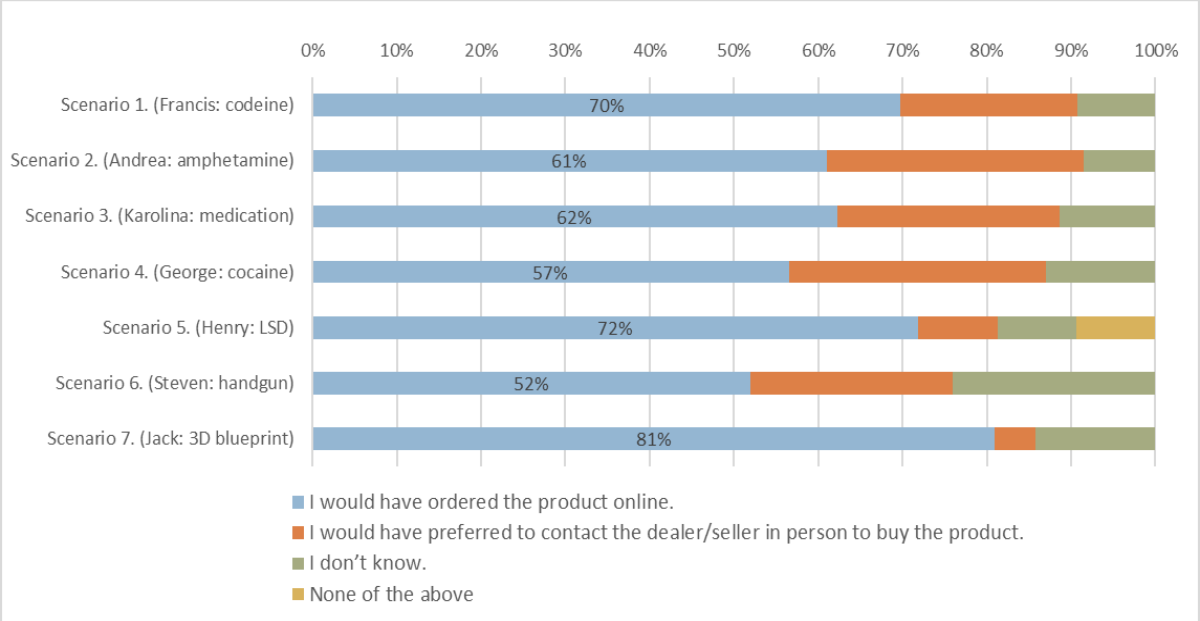

Figure E.2. Darknet survey respondents with no IT or law expertise, on where they would rather purchase products from illegally.

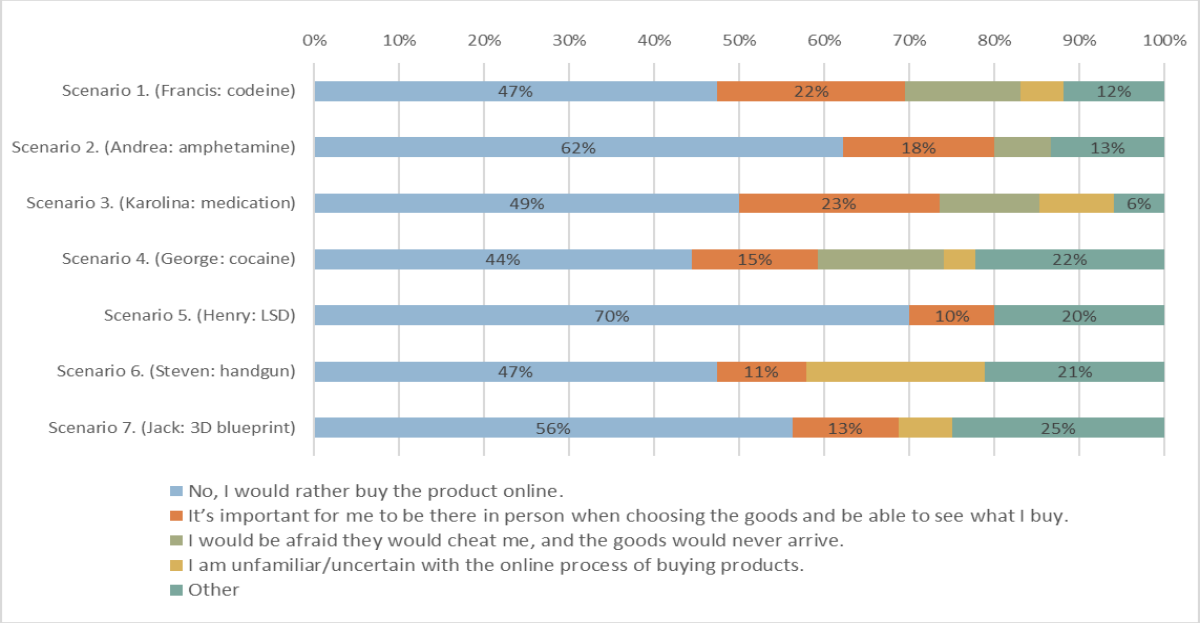

Figure E.3. Darknet survey respondents with either IT or law expertise, on preferences and reasonings for purchasing products illegally.

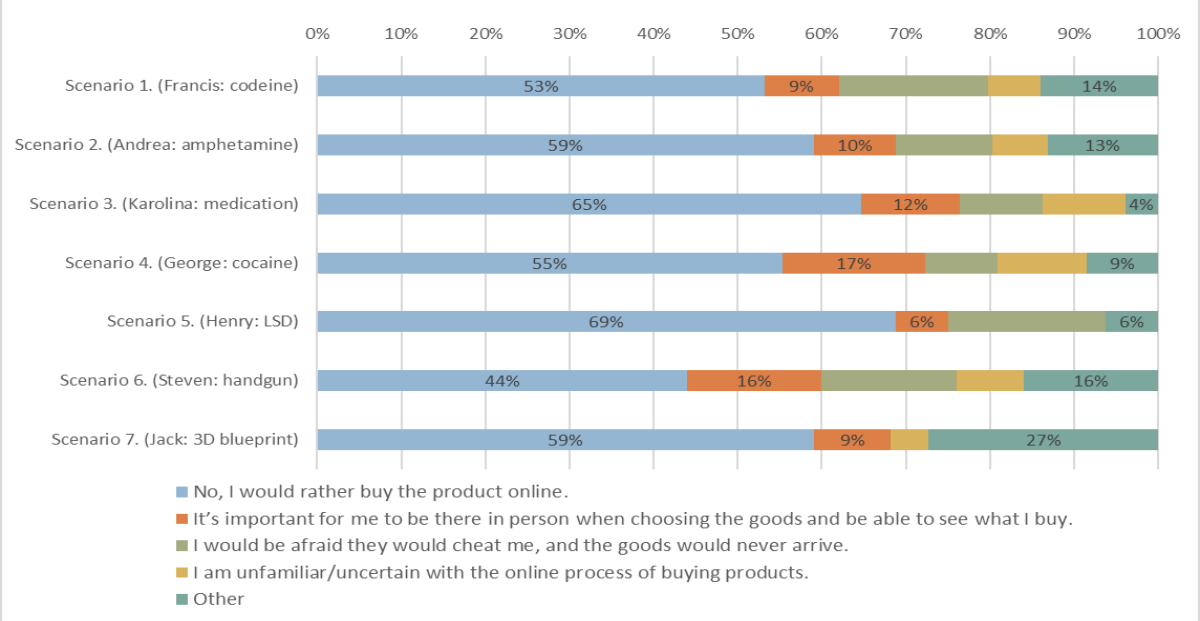

Figure E.4. Darknet survey respondents with no expertise in IT or Law, on why they would prefer online or personal meetings to purchase products illegally.

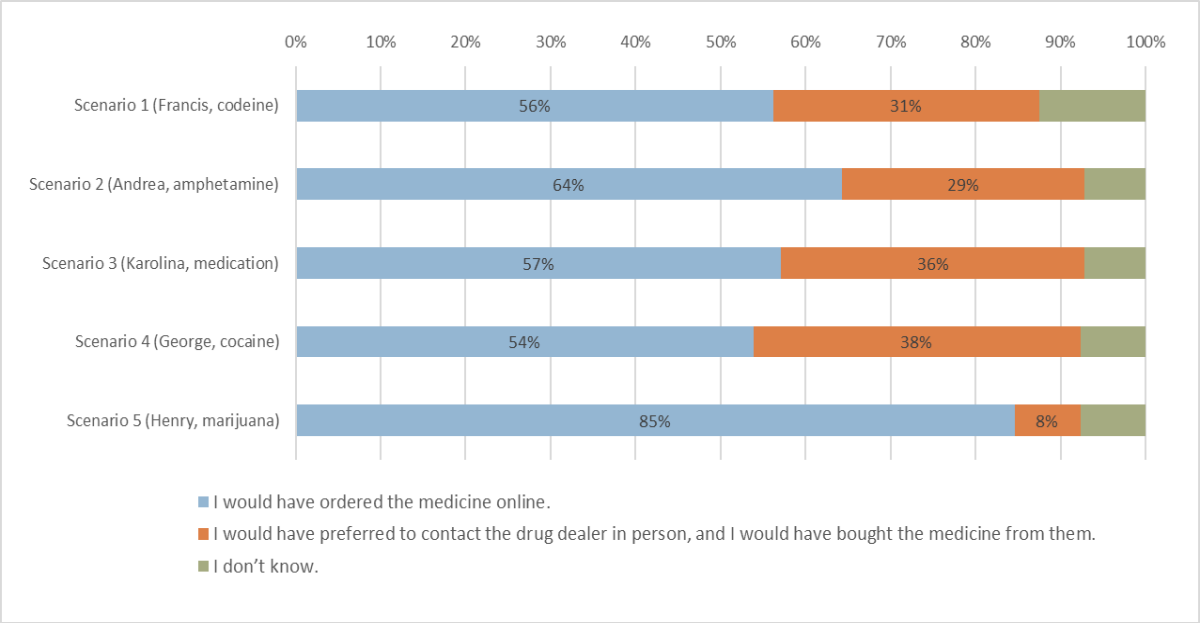

Figure E.5. University survey respondents with either IT or law expertise, on where they would rather purchase products from illegally.

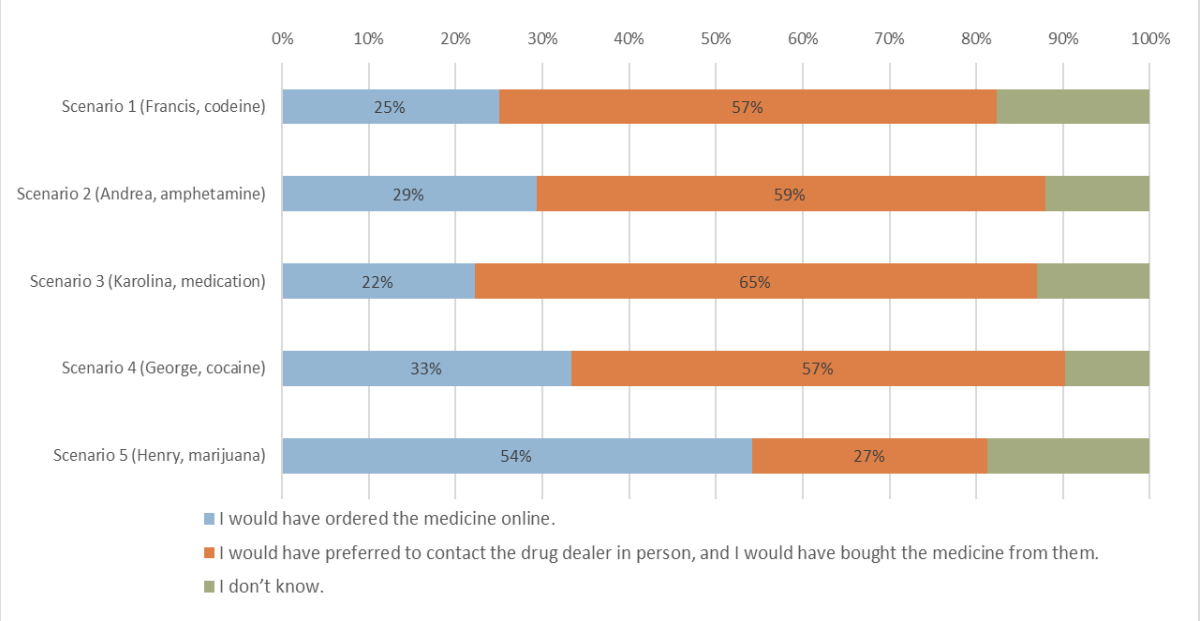

Figure E.6. University survey respondents with no IT or law expertise, on where they would rather purchase products from illegally.

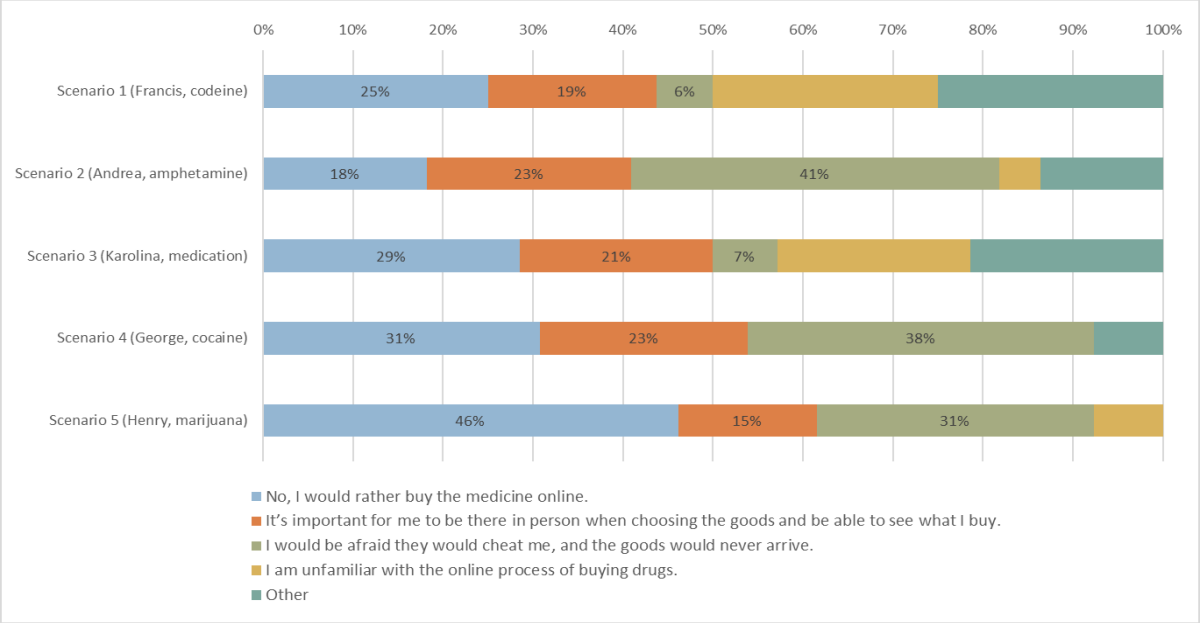

Figure E.7. University survey respondents with either IT or law expertise, on preferences and reasonings for purchasing products illegally.

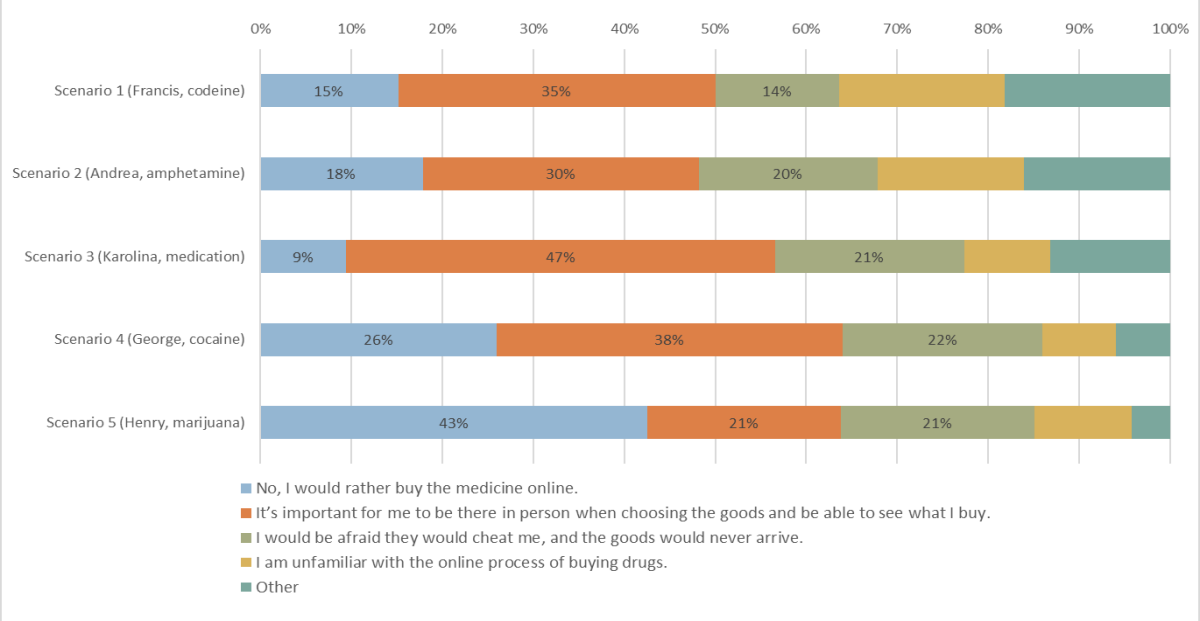

Figure E.8. University survey respondents with no expertise in IT or Law, on why they would prefer online or personal meetings to purchase products illegally.

Appendix F. Trust Matrix

Trust Factor	All scenarios		Illicit drugs		Firearms
	DarkN	Uni	DarkN	Uni	DarkN
Vendor contact and helpfulness*	**67%**	**70%**	**71%**	**66%**	**83%**
Vendor reliability*	**90%**	**86%**	**97%**	**85%**	**92%**
The popularity and positive feedback of the web store on the Internet	**76%**	63%	**81%**	61%	62%
The recommendation of the store by acquaintances or friends	38%	**70%**	45%	**67%**	15%
The web store page is easy to navigate	33%	59%	35%	58%	23%
Smooth internet connection while shopping	56%	60%	58%	55%	54%
Protection of personal and purchase data*	**87%**	**79%**	**86%**	**75%**	**92%**
Discusses the rights and obligations of buyers and vendors information	57%	58%	56%	59%	62%
The option of registering, or not, for browsing and purchases	48%	61%	54%	60%	38%
Instant response on your online payment transaction*	**73%**	**71%**	**70%**	**71%**	**85%**
Accessible, fast and easy payment transaction*	**70%**	**80%**	**75%**	**76%**	**69%**
Traditional offline payment option	15%	46%	18%	41%	8%
Payment option with cryptocurrency	**85%**	41%	**89%**	39%	**77%**
Online payment option	52%	**71%**	59%	**67%**	38%
Wide range of products and services	42%	43%	35%	44%	54%
Vendors or manufacturers of goods or services guarantee (full refund or escrow)*	**74%**	**71%**	**76%**	**69%**	**92%**
Adequate information and details about the prices, goods and services offered*	**85%**	**80%**	**88%**	**77%**	**85%**
Good quality and value for the price*	**74%**	**76%**	**74%**	**72%**	**77%**
Reliable delivery of goods*	**81%**	**86%**	**76%**	**83%**	**100%**
Opportunity to buy in a hidden and untraceable way*	**90%**	**75%**	**93%**	**69%**	**92%**
My purchase information should be deleted immediately*	**88%**	**73%**	**89%**	**68%**	**100%**
My real details should not even be known to the vendor*	**77%**	**71%**	**74%**	**67%**	**85%**

Note: Percentage of university respondents, and respondents who have been using darknet markets over one month, that answered trust factors as important across each of the scenarios. Trust factors are grouped according to trust categories; scenarios are categorized as those referring to the sale of drugs, handguns, or blueprints. Percentages above 65 are bolded to indicate a higher percentage of those who agree the trust factor is necessary.

** Indicates that respondents typically agreed that this factor was important across all scenarios.*