# Understanding Risk and Risk Perceptions of Cybercrime in Underground Forums

*Abstract*—**Understanding the reasons and the pathways of people becoming involved in cybercrime has been an important topic for research within different disciplines. Studies have explored the pathways of skilled hackers into deviant behaviour with a focus on online gaming, however little research has been conducted around understanding risk perception of cybercrime. This study investigates both surface and dark web forums, focusing on a variety of topics from hacking to gaming. The aim of this study is to a) investigate the ways cybercrime is perceived among different members of underground forums; b) identify whether there is an emotional construct of cybercrime; and c) identify the level of knowledge around behaviours which are considered as cybercrime and are criminalised. The novelty of this study lies in the methodological approach taken to conduct qualitative and quantitative research on extremely large text datasets. Our findings show different factors that can influence the thinking and decision-making process around engaging in cybercrime and online deviant behaviour. These findings also have immediate policy relevance, providing useful insights for the development of intervention approaches aiming to divert youth from being involved in cybercrime.**

***Keywords—Cybercrime, risk, perception, deviance, underground forums, natural language processing, data science***

## I. Introduction

It is well recognised that an individual's knowledge, skills and understanding of cybercrime and online deviance as well as their experiences, perceptions, attitudes and beliefs are the main influencers of their behaviour. Of these, personal motivation and personal ability are two of the most powerful sources of influence [1]. Until now it is unclear how cybercrime and online risks are perceived. While some research into perceptions of crime has been carried out, that is very limited.

Additionally, there are misconceptions about the seriousness of crime and the imposed sentences to offenders [2]. Findings show that different types of cybercrime are perceived as being less serious than non-cybercrime [3]. There is confusion regarding the law (including a perceived lack of police interest in responding to cybercrime), normalization of risky or harmful online behaviour as well as a variety of misconceptions about cybercrime alongside an ambivalence towards the potential risk of becoming a victim [4].

This study investigates both surface and dark web forums, focusing on a variety of topics from hacking to gaming. The aim of this study is to a) investigate the ways cybercrime is perceived among different members of underground forums; b) identify whether there is an emotional construct of cybercrime; and c) identify the level of knowledge around behaviours which are considered as cybercrime and are criminalised. The novelty of this study lies in the methodological approach taken to conduct qualitative and quantitative research on extremely large text datasets. In addition, this research focuses on a topic with limited existing previous research.

This paper is structured as follows. Section 2 reviews current literature on perception of offline crime as well as cybercrime. In Sections 3 and 4, we describe the data and the methodology followed. Section 5 presents the findings of the qualitative and quantitative analysis. In Sections 6 and 7 we discuss our findings and conclusions.

## II. Literature Review

### *A. Risk Perception, Emotion, and Personality*

Risk perceptions can change in different social settings based on different life events [5]. Also, not all offenders assess the costs and benefits of crime in similar ways or to similar outcomes [6]. In addition, risk taking, especially for the youth, needs to be considered based on the dynamics, the relationships, and resources around them. Most importantly, we must recognise that risk taking is integrally bound up with the development of young people's identities [7].

The behavioural decision-making framework [8] describes the process of assessing risk based on how to assess subjective probabilities (what adolescents believe) and values (what adolescents want or prefer). Fischhoff also shows how social and affective factors can have influences on behaviour via these constructs.

Another interesting model is the prototype-willingness model [9] influenced by the theories of reasoned action and of planned behaviour. According to the model, willingness appears to be a more sensitive measure than either intention or expectation. Adolescents will divulge that they are willing to engage in socially less acceptable behaviours even when they deny that they intend or expect to engage in those behaviours, and willingness is associated with a greater tendency to take risks [10].

According to prospect theory [11], human risky behaviours are underlined by two psychological parameters, contextual loss and gain framing and probability levels. Prospect theory explains the biases that people use when they make such decisions: certainty, isolation effect and loss aversion. If we consider risk taking behaviour and criminality, then we could assume that often people would rather engage in a behaviour which is less risky for a smaller reward. Similarly, people would avoid being exposed to risk by certain behaviours. For example, a negative impact of perceived risk of cybercrime has been shown on the usage of online services [12].

Based on dual information processing, people might react to risk in different ways, based on logic, analyzing risk, or reacting instinctually based on feelings about the risk [13]. According to Protection Motivation Theory

(PMT) [14] [15], environmental and personal factors are combined to pose a potential threat. The threat initiates two cognitive processes: threat appraisal and coping appraisal. Threat appraisal refers to how susceptible one feels to a threat, while the coping appraisal evaluates the various factors that are likely to ensure that one engages in a recommended response that is preventive in nature.

The threat appraisal process evaluates the factors associated with the behaviour that potentially creates danger, including the intrinsic and extrinsic rewards accompanying the actions, the severity of the danger, and one's vulnerability to the threat. The coping appraisal process evaluates one's ability to cope with, and avert, the threatened danger (self-efficacy and response efficacy), balanced with the costs (or efforts) associated with protective behaviour (response cost) [1].

Research suggests that emotion is also an orienting mechanism that directs fundamental psychological processes such as attention, memory, and information processing. It appears that people rely on general affective evaluations when considering a risk/benefit-based choice. The affective response is therefore primary, while the risk and benefit judgement is derived from it [16]. Studies have linked positive mood or emotional states to reduced risk-taking [17]. Other studies have also associated positive emotional states with increased problem-solving capacity [18], but also with increased risk taking [19]. Fear has also been identified as a component of offender decision-making, especially in relation to feelings of fear of detection [20].

Cybercrime is viewed as an emotive construct, where the primary emotion being evoked is that of fear [21]. The public perception of cybercrime is often masked in hype and unrealistic portrayals, making the issue of communicating prevention packages difficult.

Lack of experience has been associated with heightened levels of fear [22] but also fear and anxiety are enhanced due to perceptions of skilled law enforcement [23]. Experienced offenders also held the strongest views that there was little to fear from any sanction or sentence arising from official criminal justice processing [24].

Personality has also been linked to risk taking and criminal behaviour. According to the general theory of crime [25], individuals who have lower self-control are more risk-taking, short-sighted, impulsive, insensitive to other individuals and seek more easy and immediate gratification. These individuals will therefore be more likely to be involved with criminal behaviour.

### *B. Risk and Offline Crimes*

Existing literature on offline crimes have alluded to offenders' risk perception, as well as relevant strategies to minimise risks, while examining the processes and acts of specific offender groups. One framework is restrictive deterrence, which refers to strategies and methods of frequency reduction employed by offenders to minimise perceived risk of persecution [26]. Restrictive deterrence is further categorised into probabilistic and particularistic restrictive deterrence. Probabilistic restrictive deterrence refers to the possibility of offenders decreasing their frequencies of offense under the mindset that higher frequency equates to higher probability of being detected. Particularistic restrictive deterrence, on the other hand, points to a reduction in offense frequencies through rational and technical strategies [27] [28]. These two types of deterrence can precede one another or occur simultaneously [27].

The concept of restrictive deterrence is researched extensively among drug dealers. The majority of research involves interviewing former and active offenders [27] [28] [29] [30] [31]. The findings suggest four common sources of risks: (1) informants [29], (2) undercover agents [27] [29], (3) law enforcement in general [28] [30], and (4) being targets of street crimes [31]. To counter the first three sources of risks, drug dealers rely on cues from customers [27] [28] or knowledge on existing drug-related laws to minimise risk [30]. For the fourth source, drug dealers utilise direct retaliation to minimise the risk of future victimisation [31].

Other research examining offenders' process and acts also illustrate similar approaches to reduce risks. In their research on residential burglars and armed robberies, [32] found that offenders discussed criteria for target selection. For instance, offenders viewed drug dealers as suitable targets due to the unlikelihood of reporting the incident to the police [33]. When interviewing 54 auto thieves on probation, parole, or incarcerated, [23] found that offenders utilised a set of strategies to establish the illusion of normalcy via physical appearance of behaviour. These include concealing damages caused during the process and driving normally. In addition, auto thieves expressed four primary fears: (1) fear of arrest, (2) fear of victim awareness and confrontation, (3) fear of discovery by family members, and (4) fear of injury [24]. These concerns can potentially encourage offenders in adopting risk avoidance behaviours. In general, these findings illustrate the variety in risk sources and subsequent strategies to manage and avoid those risks, as well as reduce detection and consequences of crime.

### *C. Risk and Online Crimes*

A number of criminological theories could be utilised in order to understand the perception of offenders and their decision-making processes. In particular, the rational choice perspective emphasizes the importance of the offender's ability to weigh deliberately the outcomes of alternative actions and to take risks willingly [34] [35]. In addition, offenders weigh up the benefits against the perceived risk of detection or punishment, as well as their skills or equipment needed. However, the high likelihood of detection might weigh more than a harsh punishment [36]. Hutchings [37] and [38] identified that cybercrime offenders generally perceive the likelihood of being detected as low, and this holds greater weight than the harshness of available punishments. In addition, [39] found that the provision of booter services is maintained by the "easy money", with little cost in terms of time spent maintaining the sites.

Furthermore, [40] proposed the "space transition theory," a criminological theory that was explicitly designed for the application to crimes committed in cyberspace. Space transition theory provides an explanation for why otherwise law-abiding persons, who do not commit crimes in the terrestrial world, engage in cyber-criminal activities. Jaishankar [40] argues that people behave differently when they move from one space to another.

They engage in cybercrime activities because they are aware of the greatly diminished chances of becoming apprehended.

According to findings [41], hackers with a stronger preference for rational decision-making processes seem to engage in preparation, reconnaissance, and attack routines that yield higher success rates than the methods employed by others with a less pronounced preference for rational deliberations. They also engage in significantly more overall hacking attempts. It appears that they are more confident in their ability to successfully attack a target and they also employ more thoughtful attack routines that yield higher success rates. Hackers with a less pronounced preference for rational decision-making processes appear to be less confident in their ability to successfully attack targets, and they engage in fewer attempts to attack them. According to the findings, personality characteristics and the propensity to engage in risky behaviours, have a significant impact for both hacking success and the overall involvement in hacking. The study established both factors as essential dimensions of cybercrime offender typologies [41].

The Online Disinhibition Effect [42] can be also seen as a special subset of Bandura's Social Learning Theory according to which people are more likely to show behaviours that are normally under inhibition or suppression [43]. In cybercrime, many offenders only start acquiring criminal skills and planning their attack after following famous cybercriminals, in many cases hackers, as their model. Online disinhibition may unleash extreme emotions and anti-social behaviours that are rarely found in reality, including hostile language and threats. It is these negative effects that pave the way for behaviours such as cyber-bullying, privacy invasion or cyber-stalking.

Despite the existence of various theoretical models, very little research has examined risks and risk perceptions within online underground communities. These communities are crucial in understanding the cybercrime and online deviance ecosystem [44] [45] [46]. While examining risk avoidance strategies in online illegal markets, [46] found that actors in these markets tend to adjust their behaviour in order to avoid being cheated by others. Thus, this study aims to broaden the literature on risk, risk perception, and cybercrime and online deviance by examining how these concepts are discussed and perceived by members of various underground forums.

## III. Data

We propose using the CrimeBB Dataset from the Cambridge Cybercrime Centre [47], which includes data 'scraped' from several underground forums with more than 90 million posts. The scraped data includes posts from both surface and dark web forums, focusing on a variety of topics from hacking to online drugs to gaming. The posts were selected from forums that were active between 2012 and 2019. A total of 26 forums were included for this study. All forums are English-language forums, with the exception of three Russian-language forums. To generate posts relevant to the research questions, purposive sampling using several combinations of keywords were utilised. Such sampling strategy is common among qualitative studies [45] [48] and allows us to examine discourse related to risks and risk perceptions among underground forums. A total of two combinations were used for querying via Structured Query Language (SQLs):

- Combination #1: police, law enforcement, FBI
- Combination #2: getting caught, get caught

With these queries, posts containing code snippets, a long list of account information and keywords, and miscellaneous links were also selected. These posts were subsequently removed, as well as posts from the three Russian forums. In addition, posts that contained advertisements for online pharmacies and casinos, or compilation of news headlines, were removed to ensure the validity of the findings. This step resulted in the removal of a total of 15,113 posts, with 257 posts that were compilation of news headlines, 14,752 posts that were adverts for online pharmacies, and 104 posts that were adverts for casinos. Thus, the final number of posts for quantitative analyses is 143,217 posts.

## IV. Methodology

### A. Quantitative Analysis

To analyse the posts, both quantitative and qualitative methods were used. For quantitative analysis, natural language processing (NLP) method is applied to the full purposive sample to identify overarching themes in the discussion. This approach is common in existing literature on underground forums where NLP and machine learning is used to automate analysis [49] [50]. These methods are highly suitable for large datasets where manual analysis is impractical.

For this research, we identified frequent bigrams of posts from both keyword combinations. Bigrams refer to two words that occur consecutively. For example, in the sentence "I eat apple", there are two bigrams: "I eat" and "eat apple". To derive meaningful occurrences of words, the frequency of bigrams is taken into consideration, where higher frequencies mean that the second word occurs more often after the first word. In addition, we conducted analysis to identify bigrams that were more likely to occur together and function as a single word, known as collocation.

To do so, quotations, links, and content referring to images or references (e.g., [img]...[img]) were removed. The next step was to load these datasets to a pre-written program for processing forum data. Stop words, numbers and punctuations were removed to avoid the identification of commonly used words. In addition, capitalisation of text was removed, resulting in all lower-case texts. The last step is tokenisation where each word is converted into a token.

### B. Qualitative Analysis

For qualitative analysis, a modified grounded theory approach was applied to systematically examine and categorise the content of the posts [51] [52]. This methodology is common in existing research on online subcultures using web forums and online materials [44] [45] [53]. The main aim of grounded theory methodology is to generate a theoretical framework based on inductive in-depth analysis of sampled content instead of relying on existing concepts. However, for the purpose of this research, grounded theory is used to inductively identify and categorise discourse around risks and risk perceptions among cybercriminals.

To perform the qualitative analysis, posts were randomly selected from each keyword combination as it was not feasible to perform detailed manual coding on the cleaned data (143,217 posts). Coding was conducted at post-level to capture the variations in discourse.

The first stage of coding, known as open coding, is a systematic process of comparing, labeling, and grouping subjects from the selected content. These labels and codes then guide and serve as the basis for the next stage of coding [51]. During this stage, a total of 300 posts were randomly selected from the raw data files of each keyword combination. Based on the sample, a long list of labels were generated by both authors separately. These range from labels related to the format of post (e.g. the post includes a question, the post is an advice, etc.) to the expression of emotions and attitudes (e.g., don't be stupid, likelihood of being arrested/getting caught).

The next stage of coding is axial coding. During this stage, connections between the established categories are made as well as new categories are created as researchers collect and re-examine the data in order to reach theoretical saturation [51]. For this stage, 300 additional posts were selected from both keyword combinations as the original selection included posts that did not contain useful content; these posts can be categorized by the following features: a) compilation of news headlines, b) adverts for online pharmacies, and c) adverts for casinos. These mainly included random compilations of news headlines or adverts for online pharmacies. To ensure the second round of post selection would result in insightful content, a total of 15,113 posts from the aforementioned categories were removed (257 posts from Category A, 14,752 posts from Category B, and 104 posts from Category C). Both authors revisited the new sample of 300 posts and discussed the connections between labels and codes from the previous stage. This resulted in the collapse of codes from open coding into six categories.

The final stage of coding is selective coding which involves identifying a core category that encapsulates the connected categories established during axial coding [51]. Content within the six categories were re-examined and was collapsed to form one core category: risk and risk perception of cybercrime and online deviance.

## V. Findings and Results

### A. Quantitative Results

For the NLP analysis, we chose to examine the 10 most frequently occurring bigrams from each keyword combination, as shown in Table 1. We selected terms that occur together more than 500 times. It is no surprise that the top two bigrams were part of the keyword combinations for the selection of posts. Nonetheless, the discourse placed an emphasis on aspects of law enforcement such as police report and engaging with the police, as indicated by the bigrams (call, police) and (report, police). Next, to identify significant collocation, the bigrams were further filtered using the *Pointwise Mutual Information (PMI) score*. This score compares the probability of two events co-occurring with the probability of those events being independent [54]. The significant collocations provided more insight to the discourse surrounding getting caught and law enforcement.

Table 1. Top 10 Bigrams from Keyword Combinations

| **Bigrams** | **Frequencies** |
|---|---|
| getting, caught | 10,616 |
| law, enforcement | 9,899 |
| call, police | 5,856 |
| police, officer | 4,106 |
| police, report | 3,376 |
| police, station | 2,919 |
| local, police | 2,817 |
| united, states | 2,620 |
| police, officers | 2,609 |
| report, police | 2,509 |

Several different online criminal and deviant behaviors were mentioned, such as ('child', 'pornography') and the famous dark web marketplace Silk Road. With child pornography, the context of the collocation mainly pertains to warnings and advice to be careful with sexually explicit materials, as the consequences of being caught with child pornography are severe. With Silk Road, the context of most posts were reactions to its takedown as well as discussion on the investigation and techniques employed by law enforcement. In addition, the collocations ('credit', 'card'), ('bank', 'account'), ('personal', 'information') were discussed both as resources or tools for cybercrime, as well as areas to be aware of when committing any criminal or deviant act, which is detailed in Section 5. Overall, these results suggest that users on these forums partake in information and knowledge sharing to mitigate the risks of cybercrime, arrest, and detection by law enforcement.

With risk-related themes, the results highlight forum members' considerations on various aspects related to risks of being detected and caught. Some of these discussions were specific to offline crimes and deviance such as stealing or smoking marijuana in schools. Discussions relevant to risks and cybercrime range from advice on how not to get caught to views on competency and risks:

> *"well, to not get caught you have to make sure you don't log in from the same ip and make sure to clear regular cookies and flash cookies too. so that way ebay does not catch on." (Quote 1)*

> *"legal or not who cares, hide your traces and you will probably not get caught." (Quote 2)*

These posts suggest multiple factors may be at play when understanding risk perceptions of cybercrime and online deviance. For example, in the case of hacking, the risk of an act is dependent on one's technical competence as well as one's views on laws and legality of acts.

TABLE 2. SIGNIFICANT COLLOCATIONS FROM KEYWORD COMBINATIONS

| Collocation | Collocation | Collocation |
|---|---|---|
| goddess, kiss | common, sense | phone, number |
| robux, nbc | law, enforcement | last, week |
| runs, jino | white, hat | lets, say |
| grand, gangsters | php, www | accounts, found |
| silk, road | mac, address | high, school |
| child, pornography | enforcement, agencies | personal, information |
| social, engineering | money, laundering | chance, getting |
| united, states | cell, phone | bank, account |
| speed, limits | found, username | last, year |
| register, php | hard, drive | email, address |
| hacks, cheats | keep, mind | getting, caught |
| cfg, file | chances, getting | risk, getting |
| nbc, accounts | keep, logs | next, day |
| credit, card | need, speed | police, brutality |
| dark, web | last, night | real, life |

Another aspect is gaming. When examining posts related to the bigrams (public, hack) and (getting, banned), the posts were on the issues of using cheats and hacks for games and associated consequences. For example, there were posts sharing cheats with information and status of detection as well as questions from forum members asking about the likelihood of being banned when using a specific cheat or hack:

> *"You can boot 3 out of every 10 games and not get banned. If you go over 3, you will risk getting caught." (Quote 3)*

With risk and gaming cheats, our findings point to the general consensus that there is always risk with using gaming cheat and hack and users need to be ready to assume the responsibility and consequences:

> *Max Gold on 8 toons is 8mil gold, that is doable but the chance of getting caught is high. And first rule of botting is don't bot on any account you want to keep, any account with 8 90's (Assuming they are 90's to get into areas with profitable mats) I wouldn't bot with. The issue I get as a vet gold farmer of 6 years is selling my gold where did you sell yours? (Quote 4)*

These posts illustrate that some degree of appraisals are encouraged by the community prior to a decision (which is using a cheat or hack in this scenario). There is also the assumption that users are knowledgeable and aware of involved risks and the responsibility is therefore on them rather than the developers of the cheat or hack.

### *B. Qualitative Results*

In order to explore general topics deriving from our data, we used a modified grounded theory approach. There were six main types of posts that were analysed: a) comment; b) question-request; c) advice; d) instructions/tutorials; e) selling-offer; and f) giveaways. Within the core category of risk and risk perception of cybercrime and online deviance, there were several dimensions that emerged during the inductive approach: 1) risk perception, 2) perception of the criminal justice system, and 3) risk avoidance strategies. These categories provide an overview on the discussion of cybercrime perception. Representative quotes are being presented below from the randomly drawn samples when appropriate.

*1) Risk perception:* Risk perception was one of the main themes in this analysis. Within this theme we identified the following categories: a) online crime and deviant behaviour; b) perceptions around the legality of cybercrime; c) perceived likelihood and impact of detection or punishment; d) cost-benefit analysis and decision making; e) perception of the criminal justice system; and f) risk avoidance strategies.

*a) Online Crime and Deviant Behaviour:* A number of online crime and deviant behaviours have emerged through our qualitative analysis. The different types of these behaviours are presented in Table 3.

TABLE 3. ONLINE CRIME AND DEVIANT BEHAVIOUR

| **Online Crime and Deviant Behaviour** | |
|---|---|
| Doxing<br>DDoS<br>Bots<br>Cheats-exploits<br>eWhoring<br>Fake accounts<br>Fraud | Hacking<br>Impersonation<br>Malware<br>Phishing<br>RATs<br>Trolling-Harassment |

*b) Hacking:* Hacking is one of the main types of cyber-attacks identified from the analysis of our dataset. For example, hacking referred to hacking a WIFI or hacking the school system and bypassing security. In addition, posts related to the differences between white-hat hackers or black-hat hackers but also on hacking skills. For example:

> *"There's a few things you'll need to figure out. If you're going white-hat, you'll need to know if you plan to make a job out of it. If you're going black-hat, you'll need to know how easy it is for someone to find you." (Quote 5)*

*c) Gaming:* Cheating in video gaming emerged as a big theme in our analysis. Discussions were mainly identified around methods to kick people offline, sharing cheats or code in order to create an advantage beyond normal gameplay. In addition, our analysis showed a distinction between public cheats and private cheats, with private ones being considered less detectable. As mentioned:

> *"Using any of our hack tools is a pretty simple process, however we do recommend that you read all of the information on this page before operating the cheat. So our Grand Gangsters 3D hack takes advantage of a loophole in the in-app purchase system of both the Android and iOS app store, which effectively enables us to generate unlimited amounts of premium currency in just about any mobile game at 0 cost." (Quote 6)*

*2) Perceptions around the legality of cybercrime:* Our findings indicate that members of the forums we analysed, engage in discussions around the legality or illegality of certain types of actions, such as hacking or fraud. It is evident that there is a lack of understanding on the lawfulness of specific behaviours online. However, that depends on the level of experience of a forum member. Young people might not be aware of the ethical or legal boundaries of their online behaviour. While playing video games, retaliation on a component might lead to use of hacking tools and practises crossing the line of legality [55] [3]. We provide some illustrative examples of the posts below:

> *And hacking Wifi...... someone's shown they can hack the latest WPA2 encryption, by using lots of Nvida chips from graphic cards to speed up the process, but i believe this is only one way traffic that can be sniffed. So unless the police have hired uber hardware geeks that know what they're doing i wouldnt be worried ! lol (Quote 7)*

The perception of legality, risks of getting caught, and possible consequences was also discussed frequently in the context of schools. These posts suggest that some of these users were underage and at a developmental stage where risk perception differs [56]. The opinions on the risks of getting caught and possible consequences were less homogenous, as shown:

> *No you wont lol, I know countless people who have hacked schools and didn't get caught. What do you base your opinion on (Quote 8)*

> *I am a sophomore in high school and I was playing around with command prompt. It was blocked so I used the command.com edit in notepad and saved it as a .bat and everything. I tried to ddos a website and a man came in and said they had "hack" attempts. I played dumb and was all "Seriously, you need to confess". They found me and I got OSS (Out of School Suspension) for a week. Plus no phone/computer/ipod/ipad/tv/ NOTHING. :) So, it sucked and here I am. If you see something on youtube that says" How not to get caught hacking" do not believe it. (Quote 9)*

Despite the differences in personal accounts with perceived risk of hacking in school context, the more general discussion on associated risks and consequences around the behavior indicate some level of certainty with being caught:

> *Yeah man, if your school has a decent computer tech guy. You will for sure get caught. And suspended for weeks if not expelled for potentially breaching there [their] security. I would really suggest removing it. (Quote 10)*

> *Really, hacking schools computers or bypassing their security isn't worth it. You'll be lucky to get around it once if even at all. And the chances of you getting caught and punished or extremely good. Schools take computer hacking seriously. It's not worth it. (Quote 11)*

Occasionally, forum members engaged in more general discussions on rights and wrongs of these acts, sometimes drawing parallels to real-life examples:

> *"Haven't you ever heard of Ethics? It doesn't matter if you get caught or not. It is still Fraud. It is still illegal. It is still bad not not very ethical." (Quote 12)*

These posts highlight possible tension between members on their knowledge and perception on morality and legality of online crimes and deviance. Often, the distinction between acceptable and unacceptable cheating was based on harm to others, despite both actions not being allowed by most gaming platforms.

*3) Perception of the Criminal Justice System:* With the perception of the criminal justice system, the discussions largely focused on two components of the criminal justice system: law enforcement and court system. Such focus is potentially a byproduct of the sampling strategies. Nonetheless, this finding is consistent with law enforcement being seen as a source of risk in offline crimes [28] [30].

*a) Law Enforcement:* With law enforcement, our findings indicate a mixed perception towards law enforcement agencies. There were posts with news stories of successful arrests related to scams, hacking and online drug sales that show to forum members the effectiveness in law enforcement in policing cybercrime. Some of these is reinforced with posts on personal experiences or knowledge on arrests of other forum members:

> *“Blackshades is a nono, the police turned up at my house due to it.” (Quote 13)*
>
> *I mean they could do some damage and put peoples lives in danger (such as shutting down their radios or their dispatch center) but putting the public at risk isn't what Anonymous is about. Plus there's no parole in federal prison so I doubt someone's gonna be dumb enough to cyber attack the police. (Quote 14)*

Despite these personal experiences and news stories, some members remained doubtful about law enforcement’s abilities to police online crime and deviance:

> *Dude, don't stress. As long as you don't touch peoples bank accounts, CC's etc. then you're fine. It IS illegal, to have control over somebody elses computer; but the cyber police have way worse things to deal with and simply don't care enough to investigate you. There's like a 0 risk factor.(Quote 15)*

These posts suggest that members viewed the involvement of law enforcement to be low or uncertain due to limited technical capabilities or lack of knowledge on cybercrime and online deviance. Such views may affect members’ risk perception by underestimating the certainty of detection and arrest. In addition, these views are in contrast with current literature showing that constables in the United Kingdom acknowledged the uniqueness and severity of cybercrimes compared to offline offenses [57]. Such discrepancies can lead to biased appraisal of risks during the decision-making process.

Members also discuss monitoring carried out by law enforcement. With regards to monitoring by law enforcement agents on forums, the reactions and attitudes of members were mixed:

> *Hello it was 7 months ago, i got raided on discord for having some "hacker tools" 7 policemen came put all my stuff, found few usb sticks with celebrity nudes on it. laptop mobile phone everything. they accussed me of hacking their Clay Davis etc.(Quote 16)*

These posts demonstrate some level of awareness of the presence of law enforcement agents. In response, members tend to advise others to be careful with public content on forums. Alternatively, some members downplayed the importance of law enforcement presence and viewed it as an overreaction. In some instances, law enforcement involvement is used in mockery towards other members, reinforcing the notion that actions of forums members are not priorities of law enforcement agencies:

> *“It's an open discussion forum, meaning I can say just about anything I want. If you're seriously threatened by somebody on a forum, call the police, so that they can join in on the laugh I'm having right now.” (Quote 17)*
>
> *I'm sure that there are a couple on here but as I've said plenty of times the police have bigger fish to fry than the likes of us. (Quote 18)*

Other discussions on law enforcement were broader and on the topics of the rights of and regulations on access to information and data (e.g., chat history and pictures on phones) by law enforcement. These discussions are in line with current literature identifying law enforcement as a source of risk [28] [30] and members are therefore showing effort to keep up with changes in their practices.

*b) Court System:* Similar to law enforcement, members shared news stories on successful prosecutions and sentencing. These news stories covered not only the outcomes of scammers, hackers or vendors on the dark web, but also on the prosecution of buyers of drugs such as marijuana from online vendors. These stories again demonstrate to forum members that there are consequences from cybercrime. In addition, there were general discussions on the roles of online crimes and newer technologies in the court system:

> *“Ok sooo. I made a bad-ass virus. Not a script kiddie batch virus either. A totally rad super fuckyou virus. Their is this guy at my school who I reallllyy hate. So I phished his girlfriends facebook then sent him a file from her account. He downloaded and ran the virus. It killed his computer. His girlfriend found out she had been phished and took a screenshot of my phishing page and they are using it as proof against me. He called his lawyer and such so he means business. What am a facing for phishing and making and sending a virus? If the proof holds in court.” (Quote 19)*
>
> *“However, you can spoof a mac address and or change it therefore it's not even concrete enough to use in court.” (Quote 20)*

These quotes showed a focus on the admissibility of technical evidence during the prosecution procedure, both before and after an act. This is an important factor as the lack of evidence may lead to dismissal of charges, resulting in little or no consequence.

*4) Perceived likelihood and impact of detection or punishment:* A number of posts are requesting advice on the risks related to specific hacks in the online gaming environment, with the biggest worry being banned from a game or losing an account. A large number of posts also discussed the Valve Anti-Cheat (VAC), an automated anti-cheat detection system used by Steam. According to the disclaimer on the website "Any third-party modifications to a game designed to give one player an advantage over another is classified as a cheat or hack and will trigger a VAC ban." The severity of VAC bans are high as they are "permanent, non-negotiable, and cannot be removed by Steam Support" [58]. We provide some examples of the posts below:

> *"it's just that i used to do it and i always wondered what where the chances of getting caught, sometimes i really just want to kick people offline but i never dowload the software i always think what if i get caught?" (Quote 21)*

> *"if you get caught using stealth you'll get yourself a ban." (Quote 22)*

> *"Unlucky me it got banned because used several steam accounts for different games while being on the same IP/Network." (Quote 23)*

It is also possible for other players to report a player, and this can lead to being banned from a game.

> *nice job man.. but everyone know this before.. and its illegal to use fakerscript etc.. you know that they can ban u ?? (Quote 24)*

Despite the potential consequences of using cheats and hacks in games, these posts suggest that members of these forums continue to consider and/or use these cheats.

*5) Risk Avoidance Strategies:* Three types of risk avoidance strategies were identified. Each type of technique corresponds to different stages of cybercrime and online deviance. In general, the purposes of these strategies are to conceal oneself and achieve the appearance of normalcy. Concealing oneself increases the difficulties in linking an act with an individual, while appearing normal reduces the likelihood of being detected.

*a) Anonymity and Confidentiality:* Our findings show that remaining anonymous and untraceable is crucial in decreasing the chance of being detected and caught. This is present in posts on hacking, drug dealing, and gaming, albeit differences in actual techniques and approaches. For example, in an instruction for using stolen credit cards, detailed steps on obtaining background information on the target and the use of phone spoofer to conceal the identity of the carder. For online drug dealing, similar advice on increasing difficulties of traceability is given:

> *"Always change lab locations, stealth, rotate employees, open and closes front or laundering shops. Have several at the same time so you can switch work between places. Its like playing whack a mole with LE. If you stay too long in one single place, you'll get caught." (Quote 25)*

For hacking, the most common strategy for anonymity is the use of a virtual private network (VPN). The purpose of VPN is to lower the risk of being traced. This advice is frequently given when members expressed worries and fear of being caught or arrested.:

> *It's pretty simple. If you do not want to get caught, download hotspot shield. It hides your real IP Address. Or better yet, just install all your shit on a VPS, and access it on a VPN for even more security. (Quote 26)*

> *"You can go ahead and RAT your school or public places, but use a proxy and VPN to avoid being caught." (Quote 27)*

Regardless of the type of online offenses, the purpose of anonymity is to reduce the probability of being caught by increasing effort or difficulties in linking online and/or offline identities. Another strategy is to remove information or evidence that would allow for the linking of identities. Members are frequently asking for technique or method, either out of worry or in preparation for the worst-case scenario:

> *"is there a way to remove every trace? just in case you get caught or paranoia or something :P." (Quote 28)*

These questions reflect members' concerns with possible consequences (e.g., arrest) when deciding or engaging in cybercrime. It also indicates some degree of planning and preparation prior to the decision to engage in an act.

*b) Threshold:* Another risk avoidance strategy requires members to avoid a threshold. The type of threshold is dependent on the types of acts in question and is not always numerical. For example, some of these posts highlight a specific act or target to avoid in order to evade detection and/or consequences:

> *Yes it is illegal, But do they care? The answer is a simple No. Unless your cleaning Paypal's or Carding you'll be fine, If your just fucking with your victims, Opening dirty pictures & stuff, You will be fine, I dont remember the last person who called the police and said, Excuse me sir, My computer has a virus...? (Quote 29)*

> *Can you get caught? Yes. Easily? Yes. Are you going to get targeted and arrested for RATing? No.*
>
> *Probably not even for more severe cyber crimes. The only time you will get looked at is when you start pissing off people with power or money. Not just for RATing some computers. (Quote 30)*

Both posts highlight that acts leading to financial losses were more likely to lead to the involvement of law enforcement. This is related to restrictive deterrence [27] [28], as existing research has shown financial loss to be a determinant for victims to report a cybercrime [59].

*c) "Don't Be Stupid":* Another risk avoidance strategy is the use of common sense. Rather than having specific technique, members tend to warn others to not be stupid and be smart when engaging in illegal acts:

> *"Don't do daft shit, You wont get caught!" (Quote 31)*
>
> *You obviously do not live in the USA, or you don't bother reading the news. There have been over 20 publicized arrests due to small orders on silk road, and guess what? Even some vendors have been arrested, meaning all of your addresses can easily be seized and black listed, meaning if you continue ordering... you will get a knock on your door.*
>
> *Admitting to it on a public forum is no different than admitting you murdered some one. It's a federal offense that can land you in jail. Do not be so fucking stupid. (Quote 32)*

These posts demonstrate that exercising common sense and being smart is very important to minimise risk and avoid detection. This speaks to the associations between experiences, abilities and avoiding risks. In other words, if one is competent and knowledgeable, they are then exposed to very low or no risk.

## VI. Discussion

Understanding the reasons and the way people become involved in cybercrime has been an important topic for research within different disciplines. Hacking forums have been identified as an important part of the ecology since members of such forums interact with each other, share knowledge, tools and opinions. Studies have explored the pathways of skilled hackers into deviant behaviour with a focus on online gaming as a route into some forms of low-level cybercrime [60] [61].

The current study focused on understanding the perceptions and attitudes of cybercrime and the criminal justice system by different members of both surface and dark web forums. In addition, this research aimed to identify the knowledge around the criminalisation of cybercrime and the decision-making process before engaging in online deviant practises. This research is both a deep qualitative study of perceptions, attitudes, and norms, as well as a broad data science study which aims to establish these as reflective of the broader dynamics and patterns within the forum community.

The analysis identified an emerging focus around cheating in video gaming and the concerns of potential ban from a game. Cheating and game modification is increasingly used by gamers to improve their performance. These practices have led gaming networks such as Steam to set specific tactics such as VAC in order to detect cheats installed on users' computers [58]. The potential impact if detected is being banned from VAC-secured servers. Our analysis showed that the majority of forum members are concerned of such an impact, because they prefer to protect their reputation and also their access to a gaming platform. This could explain the reason why gamers, members of different forums, in this research debate the lawfulness of selling and using cheats.

In addition, our analysis showed a distinction between public cheats and private cheats, with private ones being considered as less detectable. Considering this approach via the lens of the protection motivation theory [14] [15], private cheats are a preferable method used to avert the risk of getting banned (coping appraisal process).

Hacking is one of the main deviant behaviours identified in this study. This is expected due to the type of the forums analysed. Our analysis indicates that practises such as hacking an account, a WIFI and bypassing security are being discussed by forum members based on the differences between white-hat hackers or black-hat hackers but also on hacking skills.

The legality and lawfulness of certain behaviours online such as hacking or fraud is dependent on the level of experience and ethical boundaries of forum members. As described in our analysis, the use of specific hacks is considered legal, especially when these derive from specific websites. On the contrary, practises such as selling code for hacking, online harassment as well as cracking social media accounts are considered illegal by members of the forums analysed. Therefore, these findings indicate that certain standards are set to define legality and illegality [3] [55]. This agrees with previous findings that different types of cybercrime are perceived as being less serious than others [3].

The perceived likelihood of being detected and the potential impact of certain behaviours are also discussed among forum members. In order to make decisions around cybercrime members of hacking forums follow a risk assessment process, considering the likelihood of getting caught or arrested and the potential losses versus the gains from engaging in cybercrime and online deviant behaviours. Our findings indicate a general optimistic bias influencing the perception of risk associated with cybercrime. It is a common belief among forum members that highly experienced hackers do not get caught, whereas beginners are advised to avoid risking by engaging in deviant behaviours. These findings agree with the behavioural decision-making framework [8] describing the process of assessing risk based on subjective probabilities and values. Fischhoff [8] also suggests the importance of social and affective factors in this decision-making process. This study has also identified that the emotional construct of fear is associated with deterrence of cybercrime. Discussions would clearly indicate that forum members are basing their decisions on potential fear of getting caught. But as mentioned earlier, that is mostly common for beginners, in agreement with previous studies [22].

The perception of risk of cybercrime and online deviant behaviour is also influenced by the perceptions around the criminal justice system. Our findings indicate a mixed perception towards law enforcement agencies. Some posts shared successful arrests related to hacking or scams while others indicated that there is little to fear, since law enforcement have other priorities and are not targeting low-level hackers. Overall, doubts remain among some members on the ability of law enforcement to police cybercrime and online deviance, due to their limited technical capabilities or lack of knowledge. Such views may affect members' risk perception by potentially underestimating the certainty of detection and arrest. According to findings, [24] experienced offenders held the strongest views that there was little to fear from any sanction or sentence arising from official criminal justice processing.

Our findings show a number of risk avoidance strategies being discussed. Members are frequently asking for techniques or methods, either out of worry or in preparation for the worst-case scenario. Remaining anonymous and untraceable is important for different cybercrime and online deviant behaviours in avoiding being detected and caught. A method to ensure anonymity is the use of VPN which can lower the risk of tracing an individual. Another strategy is removing information or evidence that would allow for the linking of identities. Previous studies suggest that cybercriminals need to create a balance between remaining anonymous in order to remain unseen by law enforcement and retaining certain aspects of identity in order to attract potential criminal collaborators [55] [62]. Online identities are the foundation of a cybercriminal's reputation, which provides an incentive to maintain that identity or a variation of it.

It is quite interesting also that avoiding a specific threshold which can lead to being detected is considered a risk avoidance strategy. Finally, using common sense and avoiding making common mistakes is another efficient way to avoid being detected. This agrees with the perception described earlier those skilled hackers usually do not get caught or are exposed to very low or no risk.

Future research should focus on replicating this study within a smaller number of forums to provide more detailed analyses on the accuracy and reliability of the information and strategies shared. The absence of accurate information or knowledge would allow the reallocation of resources on monitoring on these platforms. Triangulating information from online platforms with interviews of members actively engaging in cybercrime and online deviance would also identify points for intervention during the decision-making process.

Finally, we argue that the approach we have taken to this research represents a useful methodological innovation for conducting qualitative research on extremely large text datasets. Using a combination of data science and traditional qualitative methods, we took a very large database of several hundreds of thousands of posts and managed to conduct meaningful qualitative research on it. We suggest that our approach could prove useful for others attempting to do research on these large datasets of forum posts.

## VII. Conclusion

Our findings have illustrated the different factors that can influence the thinking and decision-making process around engaging in cybercrime and online deviant behaviour. These findings also have immediate policy relevance. Intervention approaches such as the one followed in the Cease and Desist program, organised by the National Crime Agency in the UK, attempt to divert youth from being involved in cybercrime. Such an approach can be informed and complemented by reviewing important factors such as the ones we observe in this study. As previous studies have shown [63] prevention measures such as warnings around the illegality of DDoS-for-hire services can halt the growth of DDoS attacks. Therefore, by increasing the likelihood or severity of punishment of such practises will increase the perceived risk and lead to successful deterrence. However, these findings need further testing and exploration.

Further approaches need to be considered such as prevention and awareness programmes taking into consideration the perception and decision-making processes around cybercrime and online deviant behaviour. Such approaches need to consider including testimonials from victims in order to portray the impact of cybercrime, but also penalties introduced for cybercrime [3].

## References

[1] M. Bada and J. Nurse, “The Social and Psychological Impact of Cyberattacks”, in Benson, V. and McAlaney, J. (eds.) Emerging Cyber Threats and Cognitive Vulnerabilities London: Academic Press, 2019, pp.73-92. doi: 10.1016/B978-0-12-816203-3.00004-6.

[2] J. Paulin, W. Searle, and T. Knaggs, “Attitudes to Crime and Punishment”, Wellington, New Zealand: Ministry of Justice, 2003.

[3] D. Kirwan, “An Investigation of the Attitudes and Environmental Factors that Make People more Willing to Participate in Online Crime”, Masters Dissertation, Technological University Dublin, 2017.

[4] G. Conway and L. Hadlington, “How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization “, Policing: A Journal of Policy and Practice, pay098, pp.1752-4512, 2018.

[5] I. Wilkinson, “Social Theories of Risk Perception: At Once Indispensable and Insufficient”, Current Sociology, 49(1), pp. 1-22, 2001. doi:10.1177/0011392101049001002

[6] D. Cornish and R. Clarke, “The reasoning criminal”, New York: Springer, 1986.

[7] E. Sharland, “Young People, Risk Taking and Risk Making: Some Thoughts for Social Work [37 paragraphs]”. Forum: Qualitative Social Research, 7(1), Art. 23, 2006. http://nbn-resolving.de/urn:nbn:de:0114-fqs0601230.

[8] B. Fischhoff, “Assessing adolescent decision-making competence”, Developmental Review, 28(1), pp. 12-28, 2008.

[9] M. Gerrard, F.X. Gibbons, A.E. Houlihan, M.L. Stock and E.A. Pomery, “A dual-process approach to health risk decision-making: The prototype-willingness model”, Developmental Review, 28(1), 29-61, 2008.

[10] V. F. Reyna and S.E. Rivers, “Current Theories of Risk and Rational Decision Making”, Dev Rev., 28(1), pp. 1–11, 2008.

[11] A. Tversky and D. Kahneman, “Advances in prospect theory: cumulative representation of uncertainty”, Journal of Risk and Uncertainty, 5(4), pp. 297–323, 1992. doi: 10.1007/ BF00122574

[12] T. Moore, R. Clayton and R. Anderson, “The economics of online crime”, J. Econ. Perspect. 23(3), pp. 3–20, 2009.

[13] S. Dickert, D. DVastfjall, R. RMauro and P. Slovi, “The Feeling of Risk: Implications for Risk Perception and Communication”, in The SAGE Handbook of Risk Communication (Thousand Oaks, CA: Sage Publications, 2015).

[14] R.W. Rogers, “A protection motivation theory of fear appeals and attitude change1”, The journal of psychology, 91(1), pp. 93-114, 1975.

[15] R.W. Rogers and S. Prentice-Dunn, “Protection motivation theory”, 1997.

[16] P. Slovic, “Trust, emotion, sex, politics, and science: Surveying the risk-assessment battlefield”, in: BAZERMAN, M. H. et al. (eds.) Environment, ethics, and behavior, San Francisco: New Lexington, pp. 277-313, 1997.

[17] P. Kusev, H. Purser, R. Heilman, A.J. Cooke, P. Van Schaik, V. Baranova, … and P. Ayton, “Understanding risky behavior: the influence of cognitive, emotional and hormonal factors on decision-making under risk”, Frontiers in psychology, 8, pp. 102, 2017.

[18] A.M. Isen, “Positive affect in decision making”, in Handbook of Emotions, eds M. Lewis and J. M. Haviland (New York: Guilford Press), 1993.

[19] B.E. Kahn and A.M. Isen, “The influence of positive affect on variety seeking among safe, enjoyable products”, Journal of Consumer Research, 20(2), 257–270, 1993. doi: 10.1086/209347

[20] P. Gill, L. Tompson, Z. Marchment, et al., “A configurative synthesis of evidence for fear in the criminal decision-making process”, Security Journal, 33(4), pp. 583–60, 2020.https://doi.org/10.1057/s41284-019-00201-w

[21] D. Wall, “Cybercrime: The Transformation of Crime in the Information Age”, Cambridge: Polity, 2007

[22] E. Beauregard and B. Leclerc, “An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making”, Sexual Abuse, 19(2), pp. 115–133, 2007.

[23] M. Cherbonneau and H. Copes, "Drive it like you stole it: Auto theft and the illusion of normalcy. British Journal of Criminology, 46(2), pp. 193–211, 2006.

[24] H. Copes and R. Tewksbury, "Criminal experience and perceptions of risk: what auto thieves fear when stealing cars", Journal of Crime and Justice, 34(1), pp. 62-79, 2011.

[25] M. Gottfredson and T. Hirschi, "A General Theory of Crime", Palo Alto, CA: Stanford University Press, 1990.

[26] J.P. Gibbs, "Crime, Punishment, and Deterrence", New York: Elsevier, 1975.

[27] B. A. Jacobs, "Crack dealers and restrictive deterrence: Identifying narcs", Criminology, 34(3), pp. 409-431, 1996a.

[28] B. A. Jacobs, "Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence", Justice Quarterly, 13(3), pp. 359-381, 1996b.

[29] B. A. Jacobs, "Undercover deception clues: A case of restrictive deterrence", Criminology, 31(2), pp. 281-299, 1993.

[30] G.J. Knowles, "Deception, Detection, and Evasion: A Trade Craft Analysis of Honolulu, Hawaii's Street Crack-Cocaine Traffickers", Journal of Criminal Justice, 27(5), pp. 443– 455, 1999. doi:10.1016/S0047-2352(99)00015-X.

[31] V. Topalli, R. Wright, and R. Fornango, "Drug dealers, robbery and retaliation. Vulnerability, deterrence and the contagion of violence", British Journal of Criminology, 42(2), pp.337-351, 2002.

[32] R. T. Wright and S. H. Decker, "Burglars on the job: Streetlife and residential break-ins", UPNE, 1994.

[33] R. T. Wright and S. H. Decker, "Armed robbers in action: Stickups and street culture", UPNE, 1997.

[34] R. V. Clarke and D. B. Cornish, "Rational Choice", in R. Paternoster & R. Bachman (Eds.), Explaining Criminals and Crime: Essays in Contemporary Criminological Theory Los Angeles: Roxbury, 2001.

[35] D. B. Cornish, "The procedural analysis of offending and its relevance for situational prevention", in R. V. Clarke (Ed.), Crime Prevention Studies (Vol. 3), Monsey, NY: Criminal Justice Press, 1994.

[36] R.V. Clarke, "Introduction. In Situational Crime Prevention: Successful Case Studies", edited by Ronald V. Clarke. Monsey, pp. 1-43, Criminal Justice Press, 1997.

[37] A. Hutchings, "Theory and Crime: Does It Compute?", Doctoral dissertation, Griffith University, Brisbane, 2013a.

[38] S.C. McQuade, "Understanding and Managing Cybercrime", Boston: Pearson Education, 2006.

[39] A. Hutchings and R. Clayton, "Exploring the provision of online booter services", Deviant Behavior, 37(10), pp. 1163-1178, 2016.

[40] K. Jaishankar, "Space Transition Theory of Cyber Crimes". In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet, pp. 281-283, Upper Saddle River, NJ: Pearson, 2008.

[41] M. Bachmann, "The Risk Propensity and Rationality of Computer Hackers", International Journal of Cyber Criminology, 4(1-2), pp. 643-656, 2010.

[42] J. Suler, "The online disinhibition effect", Cyberpsychology Behavior, 7(3), pp. 321-6, 2004. doi: 10.1089/1094931041291295. PMID: 15257832.

[43] A. Bandura and R. H. Walters, "Social learning and personality development", New York: Holt, Rinehart & Winston, 1963. 329 p. [Stanford Univ., Stanford, CA and Univ. Waterloo, Ontario, Canada].

[44] K. R. Blevins and T. J. Holt, "Examining the virtual subculture of johns". Journal of Contemporary Ethnography, 38(5), 619-648, 2009.

[45] T. J. Holt, "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures", Deviant Behavior, 28(2), pp. 171-198, 2007.

[46] T. J. Holt, O. Smirnova, Y. T. Chua and H. Copes, "Examining the risk reduction strategies of actors in online criminal markets", Global Crime, 16(2), pp. 81-103, 2015.

[47] S. Pastrana, D. R. Thomas, A. Hutchings and R. Clayton, "CrimeBB: Enabling cybercrime research on underground forums at scale", in Proceedings of the 2018 World Wide Web Conference, pp. 1845–1854, 2018.

[48] J. Miller, "The status of qualitative research in criminology", in *Workshop on interdisciplinary standards for systemic qualitative research, Michele Lamont, Arlington, Virginia*, 2005.

[49] A. Caines, S. Pastrana, A. Hutchings and P. J. Buttery, "Automatically identifying the function and intent of posts in underground forums", Crime Science, 7(1), pp. 1-14, 2018.

[50] J. Hughes, S. Aycock, A. Caines, P. Buttery and A. Hutchings, "Detecting Trending Terms in Cybersecurity Forum Discussions", in Proceedings of the Sixth Workshop on Noisy User-generated Text (W-NUT 2020), pp. 107-115.

[51] J. M. Corbin, and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria", Qualitative Sociology, 13(1), pp. 3-21, 1990.

[52] J.W. Creswell, "*Qualitative inquiry & research design: choosing among the five approaches*", Thousand Oaks, CA: SAGE Publications, Inc., 2013.

[53] T. J. Holt, "Examining the Language of Carders". In T. J. Holt, & B. H. Schell (Eds.), Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications (pp. 127-143), Hershey, PA: Information Science Reference, 2011.

[54] E.R. Aviv, Understanding pointwise mutual information in statistics, 2020. https://eranraviv.com/understanding-pointwise-mutual-information-(Accessed: 2020-06-08)

[55] J. Lusthaus, "Electronic Ghosts", Democracy: A Journal of Ideas, 31, 2014.

[56] C. White, M. Gummerum and Y. Hanoch, "Adolescents' and Young Adults' Online Risk Taking: The Role of Gist and Verbatim Representations: Adolescents' and Young Adults' Online Risk Taking", Risk Analysis. 35, pp. 1407-1422, 2015.

[57] T. J. Holt, G. W. Burruss and A. M. Bossler, "An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents", Policing and Society, 29(8), pp. 906-921, 2019.

[58] Steam Website, https://support.steampowered.com/kb/7849-RADZ-6869/ (Accessed, 25th March 2021).

[59] S. van de Weijer, R. Leukfeldt and S. Van der Zee, Reporting cybercrime victimization: determinants, motives, and previous experiences, Policing: An International Journal, 2020.

[60] R. C. Brewer, J. Cale, A. J. Goldsmith and T. Holt, "Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents". International Journal of Cyber Criminology, 12(1), pp. 115-132, 2018.

[61] S. Pastrana, A. Hutchings, A. Caines and P. Buttery, "Characterizing eve: Analysing cybercrime actors in a large underground forum", in International symposium on research in attacks, intrusions, and defenses, pp. 207-227, Springer, Cham, 2018.

[62] J. Lusthaus, "Industry of Anonymity, Inside the Business of Cybercrime", Harvard University Press, 2018.

[63] B. Collier, D.R. Thomas, R. Clayton and A. Hutchings, "Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks", in Proceedings of the Internet Measurement Conference (IMC '19), Association for Computing Machinery, New York, NY, USA, 50–64. DOI:https://doi.org/10.1145/3355369.3355592