Qualitative Criminology (QC)

Volume 14 | Number 3 Article 2

9-15-2025

Are cyber-investigators resilient in the face of adversity? An inductive qualitative analysis exploring investigators' perceptions regarding the challenges and successes in online crime police investigations

Julien Chopin
University of Lausanne

Camille Faubert
École nationale de police du Québec

David Décary-Hétu
Université de Montréal

Benoît Dupont
Université de Montréal

Jerry Ratcliffe
Temple University

Are cyber-investigators resilient in the face of adversity? An inductive qualitative analysis exploring investigators' perceptions regarding the challenges and successes in online crime police investigations

Authors

Julien Chopin, Camille Faubert, David Décary-Hétu, Benoît Dupont, Jerry Ratcliffe, and Aili Malm

Journal of Qualitative Criminal Justice and Criminology

Are cyber-investigators resilient in the face of adversity? An inductive qualitative analysis exploring investigators' perceptions regarding the challenges and successes in online crime police investigations

Julien Chopin[a], Camille Faubert[b], David Décary-Hétu[c], Benoît Dupont[c], Jerry Ratcliffe[d], and Aili Malm[e]

[a]University of Lausanne, Switzerland; [b]École nationale de police du Québec, Canada; [c]Université de Montréal, Qc, Canada; [d]Temple University, USA; [e] California State University – Long Beach, USA

ABSTRACT

Cybercrime investigations continue to pose a significant challenge for most law enforcement agencies. Specifically, these investigations present knowledge, legal, and forensic challenges that hinder police officers' ability to successfully complete their tasks and develop a sense of well-being on the job. Studies have shown that in the face of such adversity, individuals exhibit a positive coping capacity known as the resilience process. In this research, we set out to improve our understanding of both the difficulties police officers face when investigating online crimes and their ability to cope by analyzing their perceptions of success. To do this, we conducted interviews with 51 law enforcement personnel in eight countries. Our results corroborate most of the findings in extant literature, namely that the challenges faced by cyber-investigators are multilevel, and that they have developed an ability to diversify the value of their work-related successes.

JQCJC "Qualitative Criminology," (2025) Vol. 14, Iss. 3, 307-338

ARTICLE HISTORY
Received 5/24/2024
Accepted 10/21/2024

KEYWORDS
Resilience, Challenges, Success, Cyber-investigators, Online crimes

The steady increase in the number of cybercrimes in official statistics makes it inevitable that police activity will have to evolve in the near future (Chouhan, 2014; Reyes et al., 2011). Indeed, the shifts in both the number of cybercrime cases and the ever-advancing techniques used by offenders necessitate a major overhaul of how human and technological resources are used if cyber-investigators are to succeed (Choi et al., 2020; Grabosky, 2016; Nowacki & Willits, 2019; O'Kane et al., 2018). While there appears to be the political will to take up the fight against cybercrime in Western countries, many studies have reported that cyber-investigators still encounter knowledge, legal, forensic and institutional issues (Belshaw & Nodeland, 2022; Belshaw, 2019; Cummins Flory, 2016;

DOI: https://doi.org/10.21428/88de04a1.faaba6cc

CONTACT Julien Chopin (julien.chopin@unil.ch), University of Lausanne, Switzerland

De Paoli et al., 2021; Harkin et al., 2018). These issues increase the complexity of cyber-investigations, which, in turn, leads to stress, burnout, and mental health problems for cyber-investigators (Holt & Blevins, 2011; Janssens et al., 2021; Sollie et al., 2017). With respect to traditional policing, engaging in a positive coping process also known as resilience (Sollie et al., 2017) has been shown to potentially alleviate the negative aspects of police work. However, such an approach has never before been applied in the context of cyber-investigators. This qualitative study aims to assess the manifold challenges faced by cyber-investigators and identify both the use and potential of resilience as a coping mechanism.

The Four Challenges Associated with Conducting Cyber-Investigations

Previous research has shown that cyber-investigators face four different challenges when investigating cybercrimes. The *knowledge challenge* pertains to the overall lack of, or inconsistency surrounding, knowledge about cybercrimes. This is a result of the lack of an official definition for the concept of cybercrime as well as the issues involved in detecting and recording cybercrimes in official statistics (De Paoli et al., 2021). This, in turn, leads to confusion over where exactly the responsibilities of cyber-investigators begin and end, and creates a work environment that has been described as unstable due to the high turnover levels (De Paoli et al., 2021; Harkin et al., 2018; Holt & Blevins, 2011; Wilson-Kovacs et al., 2021), limited opportunities for professional development (Harkin et al., 2018; Watson & Huey, 2020; Whelan & Harkin, 2021), high workloads (Harkin et al., 2018; Wilson-Kovacs et al., 2021) and the lack of organizational commitment and recognition from senior-level management (Dodge & Burruss, 2019; Harkin et al., 2018; Wilson-Kovacs et al., 2021).

Specialists from around the world have called for the modernization of national laws that regulate cybercrimes (De Paoli et al., 2021). One of the main concerns raised by the investigators interviewed in De Paoli et al.'s (2021) study is that cybercrimes are not always punishable. The *lack or inadequacy of existing procedural laws* to deal with digital evidence is the second challenge investigators face. Most experts agree that procedural laws that were designed to regulate the police's investigative powers by focusing on physical space need to be radically revised to accommodate for the particularities of the Internet (Hinduja, 2007; Kerr, 2005; Koops, 2013). For instance, while cybercrimes often take place within one jurisdiction, the perpetrators operate from another (De Paoli et al., 2021). Acquiring criminal evidence and supporting intelligence from numerous networked devices distributed globally can be challenging for cybercrime investigators (Schreuders et al., 2020). Due to the transnational nature of most cybercrime investigations, academics argue that it requires the cooperation of police forces via mutual legal assistance treatises (MLATs) (Hinduja, 2007). However, these

types of requests take a lot of time and, hence, are nowhere near timely enough for most investigations (De Paoli et al., 2021). There are also cross-country differences with respect to public expectations towards cyber security (Schreuders et al., 2020), not to mention that some countries are simply unwilling to assist and become part of an international network (De Paoli et al., 2021).

The *forensic challenge* concerns law enforcement's lack of expertise, training, and equipment (De Paoli et al., 2021). Many staff working on investigations that involve a cyber component, across both all levels of command and national, regional and local police forces, possess a limited level of cyber knowledge and computer literacy skills (Jewkes & Yar, 2013). Due to the lack of adequate skills and knowledge, digital evidence can be overlooked, destroyed, or even misinterpreted, which raises wider concerns over the quality and scientific reliability of the services provided by forensic examiners in police agencies (Wilson-Kovacs, 2021). Moreover, while all police agencies aim to fight crime, they do not all have the same powers, resources, and roles. In this regard, distinctions are often drawn between federal, state, and local policing. As suggested by Falcone and Wells (1995, p.144), analysing and evaluating all police organisations under one homogenous model, based mainly on large, urban, municipal police departments, can lead to a "generalized misunderstanding of the organization being studied". In an analysis of officers' job stress and satisfaction in the US, Holt and Blevins (2011) noted how the availability of digital forensic expertise varies according to the size of the organisation, with larger agencies able to accommodate full-time forensic examiners, while smaller ones have officers carrying out digital forensic examiner roles in addition to their policing duties.

Finally, *recruiting and retaining staff*, specifically qualified staff, has been identified as an ongoing issue in specialised cybercrime units (De Paoli et al., 2021; Harkin et al., 2018; Whelan & Harkin, 2021). In addition to budgetary constraints, previous research has identified several factors that may have contributed to this phenomenon. First, researchers reported a lack of interest amongst police officers in taking an active role in addressing cybercrime at the local level (Dodge & Burruss, 2019; Holt & Bossler, 2012; Whelan & Harkin, 2021). Other studies found that cyber-squads were losing staff to the private sector, because the public sector simply cannot compete with private sector salaries (De Paoli et al., 2021; Harkin et al., 2018). Moreover, Whelan and Harkin (2021) reported a high turnover rate within a specialist cybercrime unit in a local police agency in Australia, which stemmed from the fact that staff were either required to leave after a set period of time or because it was the only way to secure a promotion.

Resilience Theory as a Framework for Analysing Police Work

Resilience theory is a relevant framework through which to examine how individuals deal with adversity. This theory posits that some people, acting either individually or as part of a community, are able to engage in a positive coping process to deal with difficulties (Fleming & Ledogar, 2008). Luthar (2006) presented resilience in terms of two dimensions: significant adversity and positive adaptation. According to Fleming and Ledogar (2008), resilience is never formally measured but rather is inferred from indicators related to both of these dimensions; it is important to stress here that such an approach is generally accepted by the scientific community (Masten, 2001; Sroufe et al., 2009; Yates et al., 2003). Studies converge around the idea that resilience is a process in which individuals engage depending on the presence of specific conditions (Rutter, 1990). In an attempt to extend resilience theory, Fergus and Zimmerman (2005) proposed three sub-models through which to explain resilience: the compensatory model (i.e., direct relationship between risk and protective factors), the protective model (i.e., indirect relationship between risk and protective factors), and the challenge model (i.e., curvilinear relationship between risk and protective factors). This theory derives from the field of psychology and has been applied in many different contexts, including police work (for a review, see Janssens et al., 2021). The police work context has been considered as a risky environment because of the manifold challenges it poses (Domínguez Ruiz et al., 2022; Ménard & Arter, 2014; Santa Maria et al., 2021; Sollie et al., 2017). Studies have shown that difficulties such as confrontations with crime scenes, the suffering of victims themselves as well as organisational challenges were all strong predictors of negative stress responses amongst police officers (Domínguez Ruiz et al., 2022; Janssens et al., 2021; Sollie et al., 2017). Studies have identified the presence of a resilience process amongst different police corps (e.g., crime scene investigators, uniformed patrol officers) and found that despite facing multiple adversities, they were able to engage in a process of adaptation to overcome them, manage risk factors, and improve their well-being at work (Janssens et al., 2021). The factors associated with the use of coping strategies in a resilient context has received relatively little attention. In their study of crime scene investigators, Sollie et al. (2017) identified that stress in their private life, the lack of support from colleagues, and the presence of inadequate resources were factors that hindered the development of a resilience process. Moreover, these factors increased the likelihood that crime scene investigators would engage in a negative spiral (e.g., health issues, work interruption). It is interesting to note here that police officers have been the population of choice for studying the process of resilience from various approaches; however, at least to the best of our knowledge, these studies all focused on various traditional police forces (e.g., crime scene investigators, uniformed patrol officers), and no prior research has been carried out with online crimes police investigators.

Aim of the Study

The review of extant literature results in two conclusions. First, police officers involved in online crime investigations are confronted with a significant number of challenges that are likely to induce stress, dissatisfaction and unhappiness. These challenges pertain to the definitional, legal, institutional, forensic, and structural elements of their work and are present at different stages of the work performed by investigators of online crimes. Second, previous studies have underscored that other police corps (e.g., crime scene investigators) also faced important challenges and that they engaged in a process of resilience in order to deal with them. In light of the constant evolution of online crime and the concomitant increasingly central role played by cyber-investigators, it appears important to focus on both the challenges they face and how they currently deal with them. Beyond the fundamental aspect of gaining better insight into the phenomenon of adaptability to difficulties in a work context, such an approach also sheds light on the current challenges of cyber-investigators and focuses on the protective factors they have developed to mitigate the negative consequences of their work. Consequently, this study sets out to answer two research questions:

> RQ_1: How do investigators perceive the difficulties associated with online police investigations?
> RQ_2: How do investigators adapt to the difficulties they encounter when conducting online police investigations?

Methods

Sample

To shed light on both the challenges cybercrime investigators face and their perception of their success at combatting cybercrime, we adopted an inductive approach based on interviews with cybercrime investigators and analysts employed by police agencies in different countries. Interviews were conducted with a final sample of 51 police detectives and analysts from eight different countries: Canada (n=20; 39%), the United States (n=15; 29%), the United Kingdom (n=9; 18%), Australia (n=3; 6%), France (n=1; 2%), Italy (n=1; 2%), the Netherlands (n=1; 2%) and Sweden (n=1; 2%). These specific countries were selected because the research team had previously established relationships with members of their respective police forces.

The participants were recruited via exponential non-discriminative snowball sampling. Specifically, several people were initially contacted in the different countries, and they then subsequently provided multiple referrals. We also contacted the branches

of law enforcement agencies that are responsible for the approval of research projects. Finally, because COVID-19 significantly slowed down our recruitment approach, we also turned to LinkedIn to find and contact people with the specific expertise in cybercrime investigations in public law enforcement agencies that we were looking for. This approach far exceeded our expectations, as we ultimately managed to recruit almost half of our participants (n=23/51) via this approach.

Procedure

Interviews were conducted between 5 March, 2020, and 2 September, 2021. We collected a total of 46 hours of interview content, with each interview lasting on average 55 minutes [range: 29-96 minutes]. All participants were provided with a research consent form: 46 participants gave written consent (either via email or in handwritten form), while five provided verbal consent. These five participants, who gave verbal consent, are also the ones whose interviews were not recorded. Instead, detailed notes were taken during the discussions. The decision not to record these five interviews was based on participant preference or technical limitations at the time of the interview. While every effort was made to capture the full meaning of their responses through comprehensive note-taking, it is acknowledged that relying solely on notes may limit the depth of analysis, as notes can be subject to bias and may not fully capture the nuances of participant responses. This limitation is recognized and taken into account in the interpretation of the data. Table 1, below, provides descriptive statistics of the research participants. The interviews were conducted by researchers with a background in criminology, but without direct experience in cyber-investigations. This helped ensure a level of neutrality in the interview process, reducing the potential for bias linked to prior involvement in the field. However, we recognize that researcher reflexivity is important, particularly as the analysis was performed inductively. To mitigate any influence on the interview design or participant responses, a structured interview guide was used, ensuring consistency across all interviews. While the criminological expertise of the interviewers may have shaped their approach to certain questions, their lack of direct cyber-investigative experience allowed for a more objective exploration of the participants' insights. This reflexivity was considered throughout both the interview process and the subsequent analysis to ensure the reliability of the findings.

All the interviews were divided into two sections. First, we asked participants about intervention design, as we were interested in hearing about one or two examples of police online interventions that they were involved in. We were specifically interested in understanding the triggers of these interventions, the aims, the collaborations between the public and private partners involved, the necessary resources as well as the challenges they encountered with respect to the planning and launch of the intervention.

The second section of the interviews addressed their perceptions of the impact of such interventions, as we wanted to know how the participants assessed the success of their work, the general outcomes and impacts of their interventions, the span of these impacts as well as the collateral effects of their interventions. The interview grid is provided in Appendix 1 for reference.

Table 1: Sample Description

Descriptive characteristics	*n= (%)*
Gender:	
Male	41 (80%)
Female	10 (20%)
Age (Mean):	45 years old[a] [range: 25-60]
Missing	6 (12%)
Education:	
College degree	33 (65%)
Other degree	11 (21%)
Missing	7 (14%)
Years of experience in policing:	20 years[a] [range: 3-37]
Missing	6 (12%)
Country:	
Canada	20 (39%)
United States	15 (29%)
United Kingdom	9 (18%)
Australia	3 (6%)
France	1 (2%)
Italy	1 (2%)
Netherlands	1 (2%)
Sweden	1 (2%)
Agency level:	
National	22 (43%)
Regional/state/provincial	15 (29%)
Local/municipal	11 (22%)
Missing	3 (6%)
Work status:	
Still in law enforcement	36 (71%)
Retired	11 (22%)
Quit law enforcement	4 (7%)

Notes
[a] Correspond to the mean

Analytical Strategy

The thematic analysis conducted in this research follows the guidelines proposed by Braun and Clarke (2006). First, an inductive approach was followed, which means that the data was collected without a preconceived theoretical framework (Patton, 1990). The

data collection was focused on the challenges and successes of the cyber-investigators, and it was only when later analyzing the results that the theoretical framework of resilience became relevant. Second, we sought to develop a rich description of cyber-investigators' perceptions of the challenges and successes of their investigations, as opposed to focusing on a specific aspect. Third, themes were identified at a semantic level in order to analyze the explicit meanings of the data and not look for underlying ideas. Finally, a realist/essentialist epistemological paradigm was adopted in order to obtain themes that reflected cyber-investigators' interpretations of their own experience of reality. In terms of the content analysis, a step-by-step coding process was applied to the collected data. Initially, open coding was used to break the data into meaningful segments, allowing us to identify initial themes and categories. This was followed by axial coding, where relationships between themes were explored, helping to refine and categorize the data further. Finally, selective coding was employed to identify core themes that encapsulated the central patterns emerging from the data. These steps were systematically applied using the qualitative data analysis software QDA Miner 6 to ensure consistency and rigor throughout the content analysis process. The coding process was iterative, allowing themes to be adjusted and refined as new insights emerged. The data we collected were unstructured textual data. In order to answer the research questions, qualitative data analysis QDA software was used because it has been proven to be appropriate for analyzing this kind of data (Gibbs, 2014; Peters & Wester, 2007; Talanquer, 2014). Specifically, we used QDA Miner 6 to conduct the thematic analysis and identify, group, and examine the themes addressed in a set of unstructured qualitative data (Neuendorf, 2018; Watt, 2015). To do so, continuous thematization was prioritized because it allows for themes to be modified during the course of codification (Paillé & Mucchielli, 2012). First, a vertical analysis (i.e., an intra-response analysis) was performed, which allows for both coding the responses one after the other and breaking down the data into different main themes (Gaudet & Robert, 2018). This process allowed us to develop an analytic grid, enrich it, and specify the characteristics associated with each theme (i.e., the meanings associated with the research object). Second, we performed a horizontal analysis (i.e., inter-response analysis) to identify in a transversal manner the way in which the different themes and categories were evoked in the data (Gaudet & Robert, 2018). To ensure rigor and transparency in conducting and reporting this qualitative study, we adhered to the Consolidated Criteria for Reporting Qualitative Research (COREQ; Tong et al., 2007). This checklist guided the structuring and presentation of the methodology and analysis, ensuring that all essential components were addressed, including information about the interviewers, the interview context, and data analysis procedures. The application of this checklist helps to meet high standards of quality expected in qualitative research reporting.

Ethics

This study received ethical approval from the University of Montreal. In addition, approval was obtained from the relevant branches of law enforcement agencies involved in the study. Each agency followed its own protocols for approving research projects, and permission was granted by the respective departments or units before conducting interviews. This ensured that the study complied with both university ethical standards and the specific ethical requirements of the participating law enforcement agencies.

Results

To address the research objectives of this paper, we focused on the challenges faced by cyber-investigators and their perceptions of success in their work. Through a content analysis, we identified key themes and sub-themes that can be organized into four main categories: technological and expertise challenges, organizational issues, legal obstacles, and institutional challenges. In terms of challenges, participants emphasized difficulties related to the rapid evolution of technology and the lack of specialized knowledge in cyber-investigations. Organizational issues, such as resource shortages and heavy workloads, were also frequently mentioned, along with legal challenges like jurisdictional complexities and restrictive legislation. Additionally, institutional challenges, including a lack of recognition for cyber-investigators within their agencies, posed significant barriers to their work. Regarding success, participants pointed to several measures. Judicial outcomes, such as arrests and prosecutions, were one indication of success, though disruption of criminal activities and deterrence were also seen as key achievements. The gathering of intelligence to support future investigations was another important outcome. Many participants valued the expertise gained through their investigations, and for some, the moral success of protecting victims, particularly in child exploitation cases, was considered the most significant accomplishment.

Investigation Challenges

First, we were interested in learning about both the challenges our participants encounter in their fight against cybercrime and what hinders their work. As aforementioned, we identified four categories of challenges: technological/expertise, organizational, legal, and institutional. Each are detailed below.

Technological and Expertise Challenges

Forty-three of our 51 participants (84%) raised the issue of technological challenges, mostly related to cyber-expertise. Essentially, the participants stressed that law

enforcement lacks expertise in terms of the cyber domain and the digital world, that it is a fast-paced field and that cyber-investigations are time consuming. The lack of expertise is both internal and external to cyber units. Participant #28, a cyber-investigator with experience of investigating software piracy cases for a national agency in the US, explained the lack of expertise that local and municipal police organizations face.

> In local law enforcement, you're not hiring cyber folks. They're starting to, now…. they're getting a little more but, for the most part, the local law enforcement I've seen, their cyber folks are more in the forensics part where someone, on a case, brings in a computer and they have a guy who can forensically examine. (#28)

This lack of expertise also applies to external actors, which poses a significant challenge to the work of cyber-investigators. First, many patrol officers, traditional investigators, and call centre operators are not well-versed in cybercrime, which can subsequently impact upon the work of cyber-investigators. Participant #22, a detective sergeant familiar with investigating drug sales on cryptomarkets, expressed disappointment regarding how first responders handle complex cybercrime cases. He explained that having additional investigators in his unit would not make his investigations more efficient as long as first responders do not have sufficient knowledge in cybercrime.

> I could have as many investigators….I could have 50 investigators, but the problem comes from educating first line staff or front line uniformed officers … hum …because they start … many of our investigations start … or potentially start with small digital artifacts, whether that starts from […] codes, bitcoin addresses, onion, PGP keys and they often have the lead to conduct to the money and the evidence. The officers just don't know what they are looking at. (#22)

In fact, in some instances, when faced with cybercrime cases, emergency call centre operators and front-line officers mistakenly tell victims that they do not investigate these types of crime. As a result, digital evidence can be destroyed. This agency-wide lack of knowledge of cybercrime leads to an over solicitation of cyber-investigators, which, in turn, slows down and prolongs their own cases. Participant #22 further explained that the lack of expertise from judicial actors ends up making his investigations longer because of the all the effort he has to put into explaining the investigative process and evidence type in a way that is accessible to jury members and lawyers that do not have this particular expertise.

> So resources-wise and educational wise, the scope sits, hum, beyond [the cybercrime] team. It sits beyond law enforcement officers because it's difficult for juries, hum, and lawyers to understand digital evidence that is extremely technical in nature. That leads to very long investigations. (#22)

The protracted nature of cyber-investigations largely stems from the fact that digital material is voluminous and analyzing its contents takes time. Participant #12, a Canadian investigator specializing in cases of internet child exploitation, specifically described the typical situation they encountered.

> Usually, you're looking at millions of … not specifically child exploitation material, but millions of images that you have to look through to find the evidence that you want. Hum, so that would be the next hold up … would be going through that. (#12)

Participant #50, who discussed mostly ransomware cases with us, drew an interesting contrast between the length of cybercrime investigations and the rapid changes in technologies. The roadblocks that cyber-investigators encounter are exponentially impactful when everything else around changes so quickly. For some, like participant #35, a US police officer from a regional police force, this disparity allows cyber offenders to stay ahead while law enforcement has a hard time keeping up.

> As time goes on, you have to be able to stay up with the times, because if you don't and you let it go by, then you're going to be so far behind because the criminal is always a step ahead. We have got to always stay ahead of them. (#35)

Organizational Challenges

A large proportion of the participants (82%, n=42/51) raised concerns related to the organisation of work in their respective agencies. The principal aspect reported was the lack of resources and the high workload they face. Even though some of the investigators either did not feel there was a lack of resources or recognised that the resources devoted to fighting cybercrime in police organisations had increased in recent years, the majority of the participants were crying out for additional financial, technical and human resources. Investigators #13, from Canada, and #39, from the UK both described a similar situation.

> Ultimately, you know, the … you know, as long as we have a computer and the Internet connection, we can … do something … but, yeah, absolutely, the main restriction is … personnel. (#13)

> That's really a resource issue that we're facing in the U.K. where the police numbers are being cut within the last 10 years due to austerity. (#39)

Aside from the lack of staff, the high turnover rate of cyber-investigators also poses a challenge for police organisations, mainly because of the strong competition from the private sector for these highly sought-after skills.

> The problem is, if we train people to that level and they come away with a masters' degree in whatever it might be, then they are seen as very attractive to the private companies because … Then the private companies would want to recruit our staff and we don't pay a great deal compared to those private companies. (#42)

In some cases, in which the private sector is willing to share information with law enforcement, investigators must be very cautious about using this information because, in court, they must attest to its source. When information that was obtained without a warrant or judicial authorization is shared with law enforcement, then it could end up completely ruining a case. Conversely, private companies can be bound by non-disclosure agreements that prevent them from sharing information with law enforcement.

> There are certain organizations, certain companies, out there that are just … they're real hesitant to work with law enforcement because they're afraid of alienating their customer base. (#29)

The lack of collaboration from private companies in police cybercrime investigations can prolong their duration and hamper the chances of success, which can be deeply frustrating for investigators. When legally required to provide information, private companies will ordinarily comply, but investigators might have to wait a long time for this only to find out that they did not get the information they were hoping for.

> You know how many kids have been, like, victimized while detectives or special agents are awaiting subpoena or search warrant results? […] Time could be of the essence of, like, kids being hurt, like, in the interim, which is something people never think about. […] That's my take on a lot of these companies. It's bullshit. It's all about money. (#51)

Legal Challenges

Legal challenges were raised by 78% of the participants (n=40/51) in our study. Investigators highlighted the fact that the current legislative framework is either lacking or

too restrictive in terms of fighting and preventing cybercrime. For example, some investigators noted strict legislation that restricts police investigators from committing crimes as part of their investigations. Participant #37, whose investigative work is focused mainly on internet child exploitation cases, explained the legal context in the United States that limits law enforcement investigative work.

> Part of it is the ability to collect the evidence in the first place. So, as a … in law enforcement, we are prohibited by law, from state, local, all the way up to the federal government … we can't send out or distribute child pornography, so we can't get. (#37)

Against the backdrop of increased privacy concerns and encryption software, cyber-investigators have to deal with uncooperative victims, especially when private companies are targeted by cybercrime. The lack of cooperation from victims is associated with lower reporting of cybercrime and a reduced tendency to file complaints, which prevents investigators from going further into the judicial process and conducting efficient investigations. Additionally, the most complex legal issues that cyber-investigators have to deal with are associated with jurisdictional issues. Participant #42, a cybercrime team leader in the UK who focuses on hacking cases, explained that it was one of the most complex issues he faced.

> I mean, the problems we experience with … one of the biggest problems we have is around sort of geographical resolution … What, we, in the UK, should really only be investigating breaches of law in the UK […] It's difficult for me to justify a very long investigation which could cost many hundreds of thousands of pounds if it turns out that the suspect lives in Canada and the victims are in Texas. So, it's a really difficult thing. (#42)

Participant #32 explained that extant legal procedures are so cumbersome, even with allied nations, that international investigations are incredibly complex and time-consuming. The coordination of different legal systems is challenging, so that evidence gathered in another country must respect strict guidelines in order for them to be admissible in court.

Institutional Challenges

Institutional challenges impacted upon the work of 35% (n=18/51) of our participants. They referred to aspects that pertained to both their professional identity and the ethics associated with the traditional symbol of the police and the decision-making process that aligns with it or not. Cyber-investigators expressed regret over the lack of recognition and

understanding that they feel from the rest of their agency, which gives them the impression that they must constantly advocate for themselves and the work they do in order to be deemed legitimate. Participant #20, an investigator with a specific interest in cases involving cryptocurrency, described this feeling.

> I hope that people recognize the importance of having a unit like this to … to keep the knowledge up, to understand what's going on. I don't know […] if our management understands. And I think that's the biggest hurdle for our unit … is, if our management doesn't understand what use a cybercrime unit is, or how we can help, then they could disband it because of their … ignorance, I guess. (#20)

There is a need for police agencies to adapt to the changing crime paradigm and to reconcile traditional investigative techniques with cyber-investigation strategies, which, in turn, would give more recognition to the work of cyber-investigators. According to Participant #25, this reconciliation necessitates successful partnerships, but, unfortunately, change tends to be slow in police organizations where the traditional culture is strongly ingrained.

> Partnerships, yeah, it's there and it needs to happen. And I think it's the best way for us to be successful in anything we're doing. Sadly, law enforcement, we operate in a silo, and we think we know everything and we're the very best and we have these shiny badges. […] That's very 1970s and very 1980s of us. (#25)

The ethical aspect of decision-making was also raised as a moral challenge. Given the nature of the activities that law enforcement come into contact with and focus on, investigators can find themselves in situations where the success of an investigation must be weighed-up against the additional consequences that their work could have. In relation to the aforementioned set of organisational challenges about investigators being overloaded with work and unable to investigate all the cases they come across, Participant #40, an experienced cybercrime team leader, raised the moral dilemma that this causes.

> The issue is once you find it, it is very difficult to unfind it. The senior people that created the unit are not going to be too enamored with all the resources needed to take it up, but then find somebody in Thailand or Indonesia … an individual … because there is this sort of moral obligation that you need to drill down to find out. So, that's another significant challenge with trying to police the Internet. (#40)

These words clearly show the discrepancy between traditional police operations and the moral dilemma cyber-investigators face. When patrolling a beat, police officers come across crimes that took place in their jurisdiction, but when "patrolling" the web, cyber-investigators notice crimes that happened all over the world or even that are not geographically bound. Once they "see" those cases, it becomes hard to ignore them, but agency leaders are not generally very keen to take up all the cases that happened across the globe. The strategies employed by cyber-investigators can also present moral challenges. Participant #47, while describing a large-scale operation that aimed to close platforms that hosted child sexual exploitation content and arrest the administrators, explained that some of the investigative methods they used raised moral dilemmas.

> So, because offenders, who are horrifically abusing and raping children, have taken advantage of technology and have gone to a place where they've asserted a certain effort of privacy and security, does that mean that we should allow them to do that? Does that mean that we should not proactively try to … even if that means for some period of time that we are operating the server and bad things are going to happen on the server while it's under our control. And we know that and that doesn't make any of us comfortable, you know. I mean, none of us are comfortable with that, but the alternative is to do nothing. Or just to shut it down. And then, it pops back up again. So, in an effort to cut back, to cut the head of the snake, we operate that server. (#47)

Both for the sake of the investigation's success and to prevent further victimization, law enforcement here administered the platforms for some time during the investigation. Knowing the illicit activities that were taken place during that time, investigators were uncomfortable with this fact but knew that it was necessary to ultimately bring about more good than harm.

Investigation Success

Police performance assessment is traditionally carried out by using official reported crime data. Since this metric is associated with a few caveats related to cybercrime reporting, we were interested in exploring the cyber-investigators' perceptions of the success or otherwise of their work.

Judicial Success

Most participants (51%, n=26) referred to the success of their investigations by highlighting their legal impact, such as search warrants, arrests as well as accusations

and guilty verdicts. The pride associated with legal outcomes is reflected in the words of Participant #35 below.

> I can say that in my years being in the cybercrime unit, that a lot of good was accomplished, a lot of bad people were put away. (#35)

Most of the investigators who considered arrests as a measure of an investigation's success were also cognizant that this was not the only way of measuring success. Moreover, some were acutely aware of the fact that arrests and prosecutions do not mean the end of the illicit activities.

> You know, they all get arrested, they all get done, and then new people take their places, you know and so that's what happens. But, for us, we kind of know that was going to be the end result anyway. (#36)

Others shared views of policing cybercrime that were somewhat remove from the legal impact traditionally associated with police work. On one end of the spectrum, Participant #25 explained that focusing on judicial outcomes alone can be discouraging simply because the success rates are so low.

> But if you were to take all the different cybercrime incidents, I'm sure the solvability rate is like two percent or eight percent. It would be some horrific number. And so, I think if you're looking at like prosecution rates as a sign of victory or success, then success needs to be defined quite differently in the cyberspace dimension and be more victim oriented. (#25)

At the other end of the argument, Participant #41 provided an alternative point of view grounded in the idea that it is not necessary to focus on the legal outcomes for offenders when the principal goal of the investigations is to save victims.

> I think that our group […], we were probably spearheading a lot of that work because we were measuring success in very different ways. We were looking at 'have we disrupted crime?' 'Have we managed to dismantle a network?' 'Have we managed to identify individuals enough that we can start to have a change in attitude in that space?', 'Have we scared people away from this kind of activity?'. We didn't have to prosecute to win! Prosecution is the cherry on the cake. (#41)

In the end, even though prosecutions are not always secured, these operations are nevertheless rarely not short of wins, insofar as some disruption, prevention and

deterrence almost invariably place, intelligence and expertise are gained, and lives are saved. All these aspects that must be taken into consideration are explained in the words of our participants below.

Disruption Success

Besides achieving judicial impact, police online investigations also aim to disrupt cybercrime activities. Disruption activities can have a deterrent effect, slow down the involvement of offenders in these activities and convince other potential offenders to refrain from getting involved in them. Forty-five per cent (n=23/51) of the investigators in this research raised this very point. Participant #41 cited the example below while describing the nature of his work around stopping the sales of illicit goods and services online.

> We would also run disruption activities. So, let's say there was a particular marketplace where we knew the problematic firearms or drugs or whatever were going on, we would go in and do things like leaving bad reviews for certain sellers, which would mean that they would sell less because people wouldn't buy from them anymore. (#41)

Although the array of possible disruptive and deterrent strategies employed by law enforcement is limitless, our participants raised a few ideas. For example, shutting down platforms in cases where arrests and prosecutions cannot be achieved are also potential channels of disruption and deterrence of criminal activities. Police visibility online can also manage to disrupt and deter some users. Disruption can also be achieved by prevention efforts, namely by educating and raising the awareness of both the public and industry by specifically targeting them and alerting them of their digital vulnerabilities. Participant #34 suggested educating company employees to detect phishing emails represented a starting point.

> *I think if we can … they're always going to try … criminals are always going to try … Are going to constantly try to find ways to gain money, and so, if we can educate and train some of these individuals that work for these companies or for individuals to recognise some of these fraud schemes so they don't fall for it, then we're not necessarily arresting the actor at that point, but we're preventing a victim.* (#34)

As explained by Participant #49, with regard to internet child exploitation online, prevention efforts could be oriented towards parents, communities and schools.

> By making children less vulnerable online, the activities of online child sex offenders can definitely be hampered. Basically, it's not enough to just live in this little bubble. You've got to take what you learn from there and see where it's useful and put it there as well. (#49)

All these strategies when viewed together can, ultimately, be fruitful without resorting to any type of legal action against suspects, as explained by participant #47 who was involved in investigating cases of internet child exploitation on the Darkweb.

> I think what it did is all of those successes combined have now sent a message to users that, hey, maybe the Darkweb is not as safe as I think it is … yeah, I thought it. (#47)

Criminal Intelligence Success

Success can also be assessed in terms of the amount of intelligence gathered, as noted by 27% of our participants (n=14). For these participants, even though extensive investigative efforts on their part did not lead to legal outcomes or any form of disruption of the online ecosystem they targeted, the intelligence they managed to gather was nevertheless deemed to be a marker of success. Participant #22, who has extensive experience in Darkweb investigations, explained that his ultimate goal was to identify the person who committed an online crime, even though he may be unable to arrest them for a variety of reasons.

> Success, for us, is the unmasking or uncovering of the real-world identity of the person behind the Darkweb. (#22)

The purpose of this new information is to help future investigations into other cases as well as to feed new information to other police organizations. As cybercrime pushes the boundaries of police agency jurisdiction and cross-country boundaries, police agencies must find a way to respond to this new notion of territoriality, which starts with intelligence sharing. It might sound like a consolation prize for some, but, ultimately, this information sharing is key to international cooperation in the fight against cybercrime.

> What we do know is that when there's one compromise by one bad actor, then that guy's done it hundreds of times. So, our best best in regards to solvability and getting attribution or that conviction in court, even if they're sitting in Nigeria … our best bet is for all of us across the country to take all of our individual files altogether and have a really smart person […] sit and go through all that and say: 'ahah, this person, I can tell you right now is

> sitting in Ontario and we've got them and then they're linked back to Romania because they're connected with Europol. And we've shared intelligence with Europol and connected them to Nigeria. Right? That's … that's how we're going to solve these things and deal with these geographical issues. (#25)

Expertise Acquisition

A relatively small percentage (16%; n=8) of participants explained that their measure of the ultimate impact of their work was based on gains in expertise. That is to say, whenever they considered that they had learned something from their investigation, they deemed it to be a success. Many types of learning were described by the participants, which depended on their specialisation or particular expertise. For example, participant #39 explained that every investigation represents an opportunity to learn about cyber-offenders' modus operandi, which can be beneficial for later investigations.

> So, are they [investigations] always successful? I will always try and find a positive. If you don't get a suspect, then you will always get a lesson to learn, new skills and new tactics that you aren't aware of, some new modus operandi of a criminal which helps you detect it in the future. (# 39)

Participant #36, an investigator from the UK specializing in online fraud cases, echoed this sentiment while adding that he deems investigations to be successful if they allow him to build strong relationships with financial institutions, in the case of online fraud cases.

> You know, they all get arrested. They all get done. And then, new people take their places, you know, and so that's what happens. But for us … we kind of knew that was going to be the end result anyway. But for us, it was more about building strong relationships with banks, understanding how crooks were doing things. You know, police work is always learning, you know, exercise and, you know, what can we do better next time and how do we do it next time. (#36)

This also related to developing more efficient investigative practices in the future, as explained by participant #26, a Swedish investigator inexperienced in fighting drug sales on cryptomarkets.

> One key thing that I learned is that the earlier you start with the investigation, the more likely you are to succeed because the criminals are making the

> most mistakes in the beginning. So, actually, when they set up a new marketplace, the first days or the first months are the most important to actually be very, very active as an investigator because that's the period when they make the most mistakes. The longer you wait to start your investigation, the harder it's going to be. (#26)

Moral Success

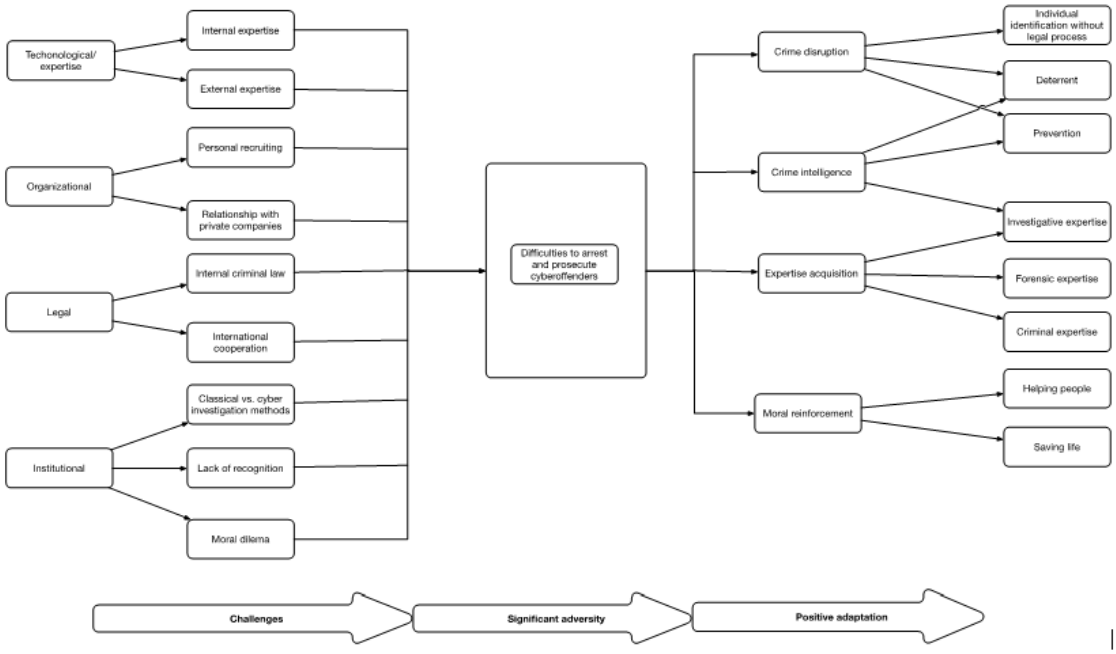
Cybercrime investigators, however, brought to our attention the fact that when legal outcomes are not possible in their cases, their job satisfaction is not limited to deterrence efforts and information gathering because helping people and saving lives is a strong component of their work in today's world in which many crimes have a cyber component. Ultimately, for 20% (n=10) of our participants, their success had a moral basis. As expressed by participant #16, this perspective is common amongst investigators focusing on internet child exploitation cases.

> I don't mean to be cliché, but it's … it's … it's rescuing one child at a time, humm … and we're talking about the most vulnerable victims that we have in the social landscape. So, you know, I think society as a whole isn't prepared to deal with the scourge of these particular minded individuals. So, I think it's … it's the satisfaction of, you know, removing at least one child from harm. (#16)

Discussion

The present study sought to identify both the challenges faced by investigators in online investigations and the way they deal with them to convert them into success. This analysis has been framed by resilience theory, which posits that individuals are able to engage in a positive coping process in order to deal with difficulties (Luthar, 2006). In the interviews, we observed that police officers involved in cyber-investigations faced considerable challenges that affected their ability to effectively complete their work of identifying and prosecuting offenders. We also identified that when faced with these challenges, investigators demonstrated a remarkable capacity for resilience by diversifying what precisely constituted success. Figure 1 summarises this resilience process, which is characterised by 1) the presence of challenges, causing 2) significant difficulties in identifying and prosecuting criminals, and leading cyber-investigators to 3) adapt positively in order to improve their well-being at work. Once again, resilience cannot be formally measured, but rather is inferred from indicators (Fleming and Ledogar, 2008), a perspective which is generally accepted by the scientific community (Masten, 2001; Sroufe et al., 2009; Yates et al., 2003).

Figure 1: Resilience Process for police Officers Involved in the Investigation of Online Crimes



When Will Meets Reality: The Multidimensional Challenges of Cyber-Investigations

The interviews we conducted revealed that police officers involved in online crimes investigations faced a significant number of constraints that made the arrest and prosecution of criminals challenging. As suggested by several authors (Holt & Blevins, 2011; Janssens et al., 2021), encountering these types of difficulties when attempting to successfully complete their duties can lead to a certain amount of unhappiness in individuals, which can be discerned in a number of indicators (e.g., stress, burnout, mental health problems). Our results are not surprising in this regard, and, indeed, are in line with previous studies on police work (e.g., Belshaw & Nodeland, 2022; Belshaw, 2019; De Paoli et al., 2021). It is interesting to observe the considerable disparity between the declared political will to intensify the fight against online crimes and the difficulties that police officers encountered at all levels to complete their task successfully (Nowacki & Willits, 2019). As previously noted, these challenges are at both macro- and micro-organizational levels (De Paoli et al., 2021; Harkin et al., 2018; Holt & Blevins, 2011; Wilson-Kovacs et al., 2021). First, legal challenges appear to be particularly constraining from investigators' perspectives, who deplore the inability of legislative authorities to

properly define their field of action, which, in turn, results in difficulties in identifying and recording these cases by the police (De Paoli et al., 2021). Furthermore, the inherent nature of these crimes, which are by definition committed outside physical borders, puts considerable strain on an international cooperation system that appears frail and challenging to mobilise (Hinduja, 2007; Schreuders et al., 2020). Second, this research also highlighted organisational problems. Unlike traditional criminality (e.g., homicide, offline sexual offending), the online nature of this crime type implies the regular confrontation between police forces and the private sector (Dodge & Burruss, 2019; Hinduja, 2007; Vincze, 2016; Wexler, 2014). The field of cybersecurity is a fast-growing business and police forces are facing stiff competition from private companies with respect to recruiting highly-skilled personnel, with whom they cannot compete salary-wise (De Paoli et al., 2021; Harkin et al., 2018). In addition, public-private sector cooperation is both urgently needed but appears to be chaotic due to legal and business issues (Dodge & Burruss, 2019). Third, our participants raised technological and expertise issues, which is in accordance with the results of previous studies (De Paoli et al., 2021; Vincze, 2016). Unlike other investigative units, the cyber-investigators in this study pointed out internal and external expertise issues. The challenge surrounding the lack of external expertise refers to the lack of specific skills and knowledge about cybercrime by first-line responders whose job it is to collect complaints from victims. The dimension surrounding internal expertise refers directly to the level of technical competence of cyber-investigators and the material made available to perform the necessary forensic investigations. Both the collection and analysis of evidence in the online crime investigation process is fundamental (Vincze, 2016) and especially time-consuming (Watson & Huey, 2020). Both the lack of expertise in the different stages of the investigative process and the lack of analytic resources evidently constitute a major challenge in terms of the identification and prosecution of individuals. Finally, it is surprising to note that cyber-investigators are confronted by challenges originating from within the police institution itself. Our participants highlighted a certain conservatism in the face of new investigative methods as well as an obvious lack of recognition of the work that they do (De Paoli et al., 2021; Jewkes & Yar, 2013). On a more individual level, certain methods used within the investigative process raised moral issues for the investigators. All of these aforesaid issues are, once again, in marked contrast with the political will to modernize the police to efficiently combat online crime (Choi et al., 2020; Grabosky, 2016; Nowacki & Willits, 2019; O'Kane et al., 2018).

There Are No Small Victories: The Resilience of Cyber-Investigators

Given all the challenges they face, the police officers in this study readily acknowledged that the success of their work is not merely about arresting and prosecuting individuals. While this, like all other crime types, was a prominent indicator of satisfaction for cyber-

investigators, the results suggest that they were able to diversify their perceptions of what constituted success when investigating online crimes. In line with Fleming & Ludogar's (2008) reflections on the concept of resilience, the combination of both significant adversity and the positive coping ability to deal with it are indicators of a resilience process. Such a finding is in accordance with previous studies examining police work through the lens of resilience (Janssens et al., 2021; Sollie et al., 2017). Although the exploratory nature of this study invites caution regarding the conclusions we might draw from our results as well as their generalizability, the findings nevertheless allow us to hypothesize that cyber-investigators demonstrate a notable ability to positively adapt themselves by engaging in a resilience process (Fleming & Ledogar, 2008). There are several specific indicators that lead us to formulate this hypothesis. First, given the difficulties in fulfilling the primary objectives of the judicial police, namely the identification and prosecution of suspects (Ratcliffe, 2011), the investigators placed value on other contributions of their work, most notably crime disruption along the criminal continuum (i.e., before and after crime commission). Specifically, the cyber-investigators valued the role that their work played in crime prevention and deterrence. The simple fact of successfully attributing a physical identity to an individual who has acted in a virtual context was perceived as a success. These successes were also largely made possible by the importance they placed upon their role in generating criminal intelligence. That is to say, the investigations they conducted, even if they did not lead to the direct arrest of suspects, provided the necessary knowledge to improve prevention strategies as well as visibility to deter crime. Second, the cyber-investigators found ways to strengthen their expertise (i.e., investigation, forensics, knowledge of criminals) from their professional experiences. Several studies have reported on the process of criminals enhancing their expertise through contact with the judicial system (Chopin et al., 2022) and it appears that the opposite also occurs. Indeed, our findings suggest that in the online crime investigation context, investigators acquire new expertise from criminals and capitalise on this to improve the handling of future cases. Finally, faced with the moral dilemmas raised by some of their practices as well as the lack of recognition from their superiors, cyber-investigators reassured themselves by developing the conviction that their work is virtuous and that, in the absence of a sufficient arrest and prosecution rate they deem to be satisfactory, they contribute to helping people and saving lives (i.e., drugs, child abuse, etc.).

Implications

Implications for Policy and Practice

Our comprehensive investigation into the challenges faced by cyber-investigators has unearthed critical barriers that hinder effective cybercrime management. These barriers

include profound gaps in necessary knowledge and expertise, outdated legal frameworks, and a glaring deficiency in technological resources. Addressing these issues is imperative to enhance the efficiency and efficacy of law enforcement operations against cybercrime. First, the rapid evolution of cybercrime methodologies necessitates equally dynamic responses from those tasked with cyber investigations. Our findings indicate that current training programs are insufficiently frequent and lack depth in content, leaving investigators unprepared for new and evolving cyber threats. To bridge this gap, law enforcement agencies should establish continuous, comprehensive training modules focused on the latest advancements in cyber threats and digital forensics. Existing training programs in areas such as counter-terrorism, financial crime, and cyber-defense could be adapted to the specific needs of cyber-investigators. These modules should include hands-on simulations, case study analyses, and lessons learned from these fields to provide real-world experience in managing complex cyber incidents. Leveraging existing training frameworks will ensure that cyber-investigators are equipped with the most relevant and up-to-date skills for tackling the evolving landscape of cybercrime. Additionally, fostering partnerships with academic institutions and private sector entities could enhance these educational programs by integrating cutting-edge research and technologies. Second, investigators frequently encounter significant delays and complications arising from outdated legal protocols that fail to reflect the current digital landscape. This includes inefficiencies in data access and cross-border cooperation due to restrictive legal statutes and cumbersome bureaucratic processes. There is a critical need for legislative reform to create agile legal frameworks that can quickly adapt to the pace of technological change. Streamlining procedures for international collaboration and updating data protection laws to facilitate quicker access to digital evidence without compromising privacy rights are essential steps. Furthermore, developing standardized cybercrime definitions and procedures across jurisdictions would reduce legal ambiguities and enhance enforcement capabilities. Third, the study highlighted a stark shortage of advanced technological tools and specialized personnel in cybercrime units. This not only strains existing resources but also contributes to high stress and burnout rates among staff, undermining their operational effectiveness. Significantly increasing investment in cyber investigation tools is crucial. This includes the acquisition of sophisticated software for cyber threat analysis, malware detection, and digital forensics. Additionally, expanding the workforce by recruiting more cyber-specialists and providing competitive compensation to attract top talent is essential for managing increased caseloads and reducing investigator fatigue. An emphasis on regular technology updates and maintenance ensures that cyber units are always equipped with the most advanced tools available.

Implications for Qualitative Criminal Justice and Criminology

The qualitative insights provided by this study underscore the critical need for a nuanced understanding of resilience among cyber-investigators. As these professionals confront the escalating complexities and evolving threats within cybercrime, understanding the interplay between their psychological resilience and the organizational context becomes imperative. Ethnographic, narrative, and case study methodologies are particularly well-suited for capturing the lived experiences of cyber-investigators, providing depth to the emotional and psychological aspects of their daily challenges. Future qualitative research should prioritize investigations into how cyber-investigators cultivate resilience amidst the stress and demands of their roles. Studies could explore adaptive coping mechanisms that investigators develop, how organizational support systems are utilized, and the role of peer networks in fostering a resilient workforce. Additionally, qualitative inquiries could examine the impact of organizational culture on resilience, identifying how leadership styles, communication flows, and team dynamics contribute to or detract from the well-being of cyber-investigators.

Implications for Quantitative Criminal Justice and Criminology

From a quantitative perspective, this research emphasizes the need for developing new metrics and models that can quantitatively assess the resilience of these professionals. Developing robust, data-driven models to measure and enhance resilience can provide actionable insights, leading to more effective strategies in combating cybercrime. Future research should prioritize the development of validated metrics and interventions aimed at enhancing the resilience of cybercrime investigation units. Quantitative approaches, such as resilience assessment tools and outcome measures, can provide valuable insights into the effectiveness of resilience-building programs. Existing tools, such as the Connor-Davidson Resilience Scale (CD-RISC), which measures an individual's ability to bounce back from adversity, and the Brief Resilience Scale (BRS), which assesses the ability to recover from stress, could be adapted for cybercrime investigators. The Cyber Resilience Review (CRR), developed for evaluating resilience in critical infrastructure organizations, may also be relevant for adapting resilience metrics in law enforcement settings. Using these tools to investigate factors such as stress management, coping mechanisms, and adaptability in high-pressure environments would be crucial in developing predictive models that reflect the unique challenges faced by cybercrime investigators. Tailoring these tools to the specific operational context of cyber-investigations would enhance their effectiveness in guiding resilience-building programs. Quantitative analyses can identify key determinants of resilience, such as coping mechanisms, social support networks, and organizational culture, allowing for targeted interventions. Moreover, longitudinal studies tracking changes in resilience levels over

time may be essential for understanding the dynamic nature of resilience among cybercrime professionals.

Conclusions

In 2014, the Police Executive Research Forum noted the fact that the American government had prepared federal agencies to address cybercrime, but that the 18,000 local agencies within the country had no plan to join the effort. In our study that aimed to identify differences in cyber-investigators' perceptions of the challenges and successes in their work, we observed that determining the success of cybercrime investigations is far from straightforward, and that one encounters many roadblocks when trying to do so. However, our results suggest that despite the challenges they face, online crime investigators are resilient and have developed a significant ability to value other outcomes of their work than mere judicial success. Indeed, while legal outcomes were the principal focus of several of the participants, which is in line with the policing tradition, many reported that overly focusing on these legal proceedings detracts from several other metrics of success that have a place in the fight against cybercrime, such as, for example, saving victims, disrupting illicit activities, preventing crime, gathering intelligence and learning.

Although this study is innovative and sheds light on important aspects of policing, a number of limitations must be acknowledged. First, it is important to note that this research was grounded in a qualitative research design, and, as such, we cannot fully discount the fact that these results are only relevant to the sample we interviewed and therefore not generalizable to all cyber-investigators. Similarly, the results derive from interviews with police officers from eight specific countries and it is not possible to generalize their perceptions to police officers from different countries. Third, we did not analyze the results in terms of the individual status of the interviewees or the level of the agency to which they belong. Consequently, we cannot exclude that these elements may have influenced their perceptions. Additionally, some participants were retired or no longer active as cyber-investigators at the time of the interviews, and given the rapid evolution of technology, their experiences may not fully reflect current practices in cyber-investigations. This factor, along with the absence of an analysis based on employment status, could have an impact on the relevance of their insights in the context of recent technological advancements. Fourth, one limitation of the study is the reliance on notes rather than audio recordings for five participant interviews, which may have affected the depth and accuracy of data interpretation. While detailed notes were taken, this approach can introduce bias and may not fully capture the nuances of participant responses, potentially limiting the richness of the analysis. Finally, our analysis of the resilience process is a purely exploratory approach based on the identification of a significant

adversity and a positive adaptation. Although this approach is commonly used, we believe that a complementary analysis based on more detailed indicators would also be useful to corroborate these results.

References

Belshaw, S., & Nodeland, B. (2022). Digital evidence experts in the law enforcement community: Understanding the use of forensics examiners by police agencies. *Security Journal, 35*(1), 248-262.

Belshaw, S. H. (2019). Next generation of evidence collecting: The need for digital forensics in criminal justice education. *Journal of Cybersecurity Education, Research and Practice, 2019*(1), 3.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Choi, K.-S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 27-43). Springer.

Chopin, J., Paquette, S., & Fortin, F. (2022). Geeks and newbies: Investigating the criminal expertise of online sex offenders. *Deviant Behavior*, 1-17.

Chouhan, R. (2014). Cyber crimes: Evolution, detection and future challenges. *IUP Journal of Information Technology, 10*(1), 48.

Cummins Flory, T. A. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law, 11*(1), 4.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice, 15*(2), 1429-1445.

Dodge, C., & Burruss, G. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. In *The human factor of cybercrime* (pp. 339-358). Routledge.

Domínguez Ruiz, I. E., Rué, A., & Jubany, O. (2022). Police Resilience as a Multilevel Balance: Needs and Resources for Victim Support Officers. *Police Quarterly*, 10986111221111322.

Falcone, D. N., & Wells, L. E. (1995). The county sheriff as a distinctive policing modality. *American Journal of Police*. *14*(3/4), 123-149.

Fleming, J., & Ledogar, R. J. (2008). Resilience, an Evolving Concept: A Review of Literature Relevant to Aboriginal Research. *Pimatisiwin, 6*(2), 7-23.

Gaudet, S., & Robert, D. (2018). *A journey through qualitative research: From design to reporting*. SAGE Publications Ltd.

Gibbs, G. R. (2014). Using software in qualitative analysis. *The SAGE handbook of qualitative data analysis*, 277-294.

Grabosky, P. (2016). The evolution of cybercrime, 2006–2016. In Cybercrime through an interdisciplinary lens (pp. 29-50). Routledge.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. Police Practice and Research, 19(6), 519-536.

Hinduja, S. (2007). Computer crime investigations in the United States: leveraging knowledge from the past to address the future. International Journal of Cyber Criminology, 1(1), 1-26.

Holt, T. J., & Blevins, K. R. (2011). Examining job stress and satisfaction among digital forensic examiners. Journal of Contemporary Criminal Justice, 27(2), 230-250.

Janssens, K. M., van der Velden, P. G., Taris, R., & van Veldhoven, M. J. (2021). Resilience among police officers: a critical systematic review of used concepts, measures, and predictive values of resilience. Journal of Police and Criminal Psychology, 36(1), 24-40.

Jewkes, Y., & Yar, M. (2013). Handbook of internet crime. Routledge.

Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Colum. L. Rev., 105, 279.

Koops, B.-J. (2013). Police investigations in Internet open sources: Procedural-law issues. Computer Law & Security Review, 29(6), 654-665.

Luthar, S. S. (2006). Resilience in development: A synthesis of research across five decades. In D. Cicchetti & D. J. Cohen (Eds.), Developmental Psychopathology: Risk, Disorder, and Adaptation (pp. 740–795). Wiley.

Masten, A. S. (2001). Ordinary magic: Resilience processes in development. American Psychologist, 56(3), 227.

Ménard, K. S., & Arter, M. L. (2014). Stress, coping, alcohol use, and posttraumatic stress disorder among an international sample of police officers: does gender matter? Police Quarterly, 17(4), 307-327.

Neuendorf, K. A. (2018). Content analysis and thematic analysis. In Advanced research methods for applied psychology (pp. 211-223). Routledge.

Nowacki, J., & Willits, D. (2019). An organizational approach to understanding police response to cybercrime. Policing: An International Journal. *43*(1), 63-76.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. Iet Networks, 7(5), 321-327.

Paillé, P., & Mucchielli, A. (2012). Chapitre 11: L'analyse thématique. In *Collection U*, (pp. 231-314).

Patton, M. Q. (1990). Qualitative evaluation and research methods (Sage, Ed. 2nd ed.).

Peters, V., & Wester, F. (2007). How qualitative data analysis software may support the qualitative analysis process. Quality & Quantity, 41(5), 635-659.

Ratcliffe, J. H. (2011). Intelligence-led policing. Environmental Criminology and Crime Analysis, 6, 263-282.

Reyes, A., Brittson, R., O'Shea, K., & Steele, J. (2011). Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors. Elsevier.

Rutter, M. (1990). Psychosocial resilience and protective mechanisms. In A. S. Masten, D. Cicchetti, K. H. Nüchterlein, & S. Weintraub (Eds.), Risk and Protective Factors in the Development of Psychopathology (pp. 181–214). Cambridge University Press.

Santa Maria, A., Wolter, C., Gusy, B., Kleiber, D., & Renneberg, B. (2021). Reducing work-related burnout among police officers: The impact of job rewards and health-oriented leadership. The Police Journal, 94(3), 406-421.

Schreuders, Z. C., Cockcroft, T., Butterfield, E., Elliott, J., Soobhany, A. R., & Shan-A-Khuda, M. (2020). Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force. International Journal of Cyber Criminology, 14(1), 316-340.

Sollie, H., Kop, N., & Euwema, M. C. (2017). Mental resilience of crime scene investigators: How police officers perceive and cope with the impact of demanding work situations. Criminal Justice and Behavior, 44(12), 1580-1603.

Sroufe, L. A., Egeland, B., Carlson, E. A., & Collins, W. A. (2009). The development of the person: The Minnesota study of risk and adaptation from birth to adulthood. Guilford Press.

Talanquer, V. (2014). Using qualitative analysis software to facilitate qualitative data analysis. In Tools of chemistry education research (pp. 83-95). ACS Publications.

Tong, A., Sainsbury, P., & Craig, J. (2007). Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. *International Journal for Quality in Health Care*, *19*(6), 349-357.

Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), 183-194.

Watson, C., & Huey, L. (2020). Technology as a source of complexity and challenge for special victims unit (SVU) investigators. International Journal of Police Science & Management, 22(4), 419-427.

Watt, A. (2015). QDA Miner 4.0. Qualitative Research Journal. *15*(2), 250-251.

Wexler, C. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime*. Police Executive Research Forum.

Whelan, C., & Harkin, D. (2021). Civilianising specialist units : Reflections on the policing of cyber-crime. Criminology & Criminal Justice, 21(4), 529-546.

Wilson-Kovacs, D., Rappert, B., & Redfern, L. (2021). Dirty Work? Policing Online Indecency in Digital Forensics. The British Journal of Criminology. *62*(1), 106-123.

Yates, T. M., Egeland, B., & Sroufe, L. A. (2003). Rethinking resilience: A developmental process perspective. In S. S. Luthar (Ed.), *Resilience and vulnerability: Adaptation in the context of childhood adversities* (pp. 243-266). Cambridge University Press.

Funding

This paper is part of the research project '*Disrupting the Darknet: Law Enforcement and their Impact of Darknet Offenders*' and funded by PMI IMPACT. The grant does not have a grant number.

Ethical Considerations

This study received ethical approval (# CERSC-2019-111-D) from the Research Ethics Committee - Society and Culture of the University of Montreal.

Acknowledgments

We express our sincere gratitude to the institutions and individuals who contributed significantly to the research presented in this manuscript. We are indebted to all the law enforcement personnel across the eight countries who participated in our study. Their insights and experiences were invaluable and have greatly contributed to the depth and breadth of this research. We also extend our gratitude our colleagues who provided expert advice and feedback during the initial drafting and subsequent revisions of this manuscript. Their critiques and suggestions were instrumental in refining our analysis and enhancing the overall quality of our work.

Contributors

Julien Chopin, Ph.D., is a senior researcher at the School of Criminal Justice of the University of Lausanne. He is also an adjunct professor at Laval University and Simon Fraser University His research focuses on sexual offending, homicide, victimology, criminological theories, criminal justice systems, and intimate partner violence.

Camille Faubert has a Ph.D. in criminology from the Université de Montréal. She is currently a researcher at the École nationale de police du Québec. Her Ph.D. thesis focused on the training of law enforcement officers.

David Décary-Hétu, Ph.D., is an associate professor at the School of Criminology of the Université de Montréal, as well as the Chair of the Darknet and Anonymity Research Centre. His research focuses on the impact of technology on crime.

Benoît Dupont, Ph.D., is a professor at the School of Criminology of the Université de Montréal. Benoit has two Canadian Chairs of Research on cybersecurity and the prevention of cybercrimes. He is also the Scientific Director of the Human-Centric Cybersecurity Partnership that was founded in 2021

Jerry Ratcliffe, Ph.D., is a professor at the Department of Criminal Justice of Temple University. He has written numerous books on intelligence-led policing and has experience both as a law enforcement officer and as a researcher.

Aili Malm, Ph.D., is a professor at the School of Criminology of the Criminal Justice and Emergency Management College at the California State University—Long Beach. Her research focuses on police and the analysis of crime through social network analysis. Aili has been involved in numerous studies on law enforcement practices.