ISSN 1411-3813 | E-ISSN 2684-7191
DOI: 10.46976/litbangpolri.v27i3.248

Emulating Police Interaction Ritual in Cyberspace: Apparent Challenge in Policing the Internet

Hafiz Prasetia Akbar[1]
[1]*Sekolah Tinggi Ilmu Kepolsian*
hafiz.prasetia.akbar@polri.go.id

ABSTRACT

As internet usage becomes increasingly relevant in daily life, the police has an obligation to have a presence, protect, and uphold the law in the digital world. However, this digital realm comprises new 'spaces' that contest traditional conceptions of physical space, wherein law enforcement has been deterring and combating crime through micro-level, direct contacts between police and the public. This paper seeks to understand the challenges encountered by police in establishing a presence in the intangible cyberspace. This study does a comprehensive literature analysis to examine the adaptation of policing methods, including interaction with the community, patrols, surveillance, and community policing, as they pertain to the cyber realm. We examine the use of established crime prevention theories, such as Routine Activity Theory, in the context of designing approaches to prevent cybercrime. The primary challenges encountered encompass the necessity of upholding legitimacy, traversing jurisdictional boundaries, and the ethical implications of employing cyber-policing. Ultimately, when faced with the challenges of existing in an abstract realm, law enforcement must continually adjust to the evolving environment while upholding the ideals that characterize policing as actions that reinforce social order.

Keyword*:* crime prevention, cybercrime, cyber-policing, cyberspace, interaction ritual.

ABSTRAK

Seiring dengan semakin maraknya penggunaan internet dalam kehidupan sehari-hari, polisi memiliki kewajiban untuk hadir, melindungi, dan menegakkan hukum di dunia digital. Namun, ranah digital ini mencakup 'ruang' baru yang menentang konsepsi tradisional tentang ruang fisik, di mana penegakan hukum telah menghalangi dan memerangi kejahatan melalui kontak langsung tingkat mikro antara polisi dan masyarakat. Penelitian ini berupaya memahami tantangan yang dihadapi polisi dalam membangun kehadiran di dunia maya yang tidak berwujud. Studi ini melakukan analisis literatur yang komprehensif untuk mengkaji adaptasi metode kepolisian, termasuk interaksi dengan masyarakat, patroli, pengawasan, dan pemolisian komunitas, serta relevansi metode tersebut di ranah siber. Teori-teori pencegahan kejahatan Teori Pilihan Rasional, Teori Deteren, dan Teori Aktivitas Rutin digunakan dalam konteks merancang pendekatan untuk mencegah kejahatan siber. Tantangan utama yang dihadapi mencakup perlunya menegakkan legitimasi kepolisian, melintasi batas yurisdiksi, dan implikasi etis dari penerapan kepolisian siber. Pada akhirnya, ketika dihadapkan dengan tantangan hidup di dunia yang abstrak, penegakan hukum harus terus menyesuaikan diri dengan lingkungan yang terus berkembang sambil menjunjung tinggi cita-cita yang mencirikan kepolisian sebagai tindakan yang memperkuat ketertiban sosial.

Kata Kunci*: pencegahan kejahatan, kejahatan siber, pemolisian siber, ruang siber ritual interaksi.*

INTRODUCTION

In urban spaces, the presence of a uniformed police officer walking a beat or patrolling in a cruiser serves as an evident indicator that a capable guardian is upholding safety and maintaining social order. The visible police presence is designed to deter criminal activity, based on the rationale that potential offenders are less inclined to commit crimes when they recognize an increased likelihood of apprehension. Such observations are not merely anecdotal; they resonate with established criminological theories that underscore the significance of policing in crime prevention. The Routine Activity Theory (Cohen & Felson, 1979) strongly believes that criminal opportunity can only occur when an offender, a suitable victim, and the absence of a ‘capable’ guardian (e.g., police officers) are together. Thus, a visible police presence has been believed to serve as a

scarecrow to deter potential criminals. Additionally, the Criminal Deterrence Theory (Beccaria, 1986) contends that the certainty of enforcement, as evidenced by a visible presence of authority, will diminish the probability of deviant behavior. Similarly, Rational Choice Theory (Clarke, 1997, p. 10) emphasizes the calculative nature of human decision-making. Offenders assess the costs and benefits of their actions, perceiving a greater risk of committing crimes in the presence of policing. Together, these theories highlight a shared conclusion: police presence significantly influences situational dynamics that deter and prevent crime. Scholars such as Jackson & Bradford (2009) supports this idea, as visible uniformed presence in physical space will signify that crime is forecasted and suppressed and society's order has been maintained. As a result, it has been clear that policing discourse has been dominated by the idea of being present in the physical world (Ericson & Haggerty, 1997, p. 137).

Dau et al. (2021) define police presence as a structural aspect, "Where and when they police, how many officers are present, how long they are present. It describes social, spatial, and temporal aspects of police work, which can be measured as definite quantities." However, as complex networks of computer technology and data systems have emerged, it has become evident that new 'spaces' have been constructed that are irrelevant to old conceptions of what constitutes physical space (Huey, 2002, p. 244). Spaces on the internet, such as social media, are online locations where users create identities and disclose personal information with one another; indeed, the entire purpose of being on social media is to create the illusion of being there, forming what is known as cyberspace. Therefore, social media has established itself as a de-facto place for interpersonal sociality, making the user visible in identity and interactions (Beer & Burrows, 2007).

Additionally, social media has become a part of the social construct that defines everyday life. According to a survey in July 2024 by Statista (2024), approximately 5.35 billion people have access to the internet, comprising around 66% of the roughly 8 billion global population. The number of internet users will rise to 7.9 billion by 2029. Approximately 95% of internet users engage with social media, with the average user spending roughly two and a half hours every day. Police organisations have thus prioritised social media presence to adapt to a transparent digital era and police the unregulated space against the possibility of information distortion (College of Policing, 2020). While it is up to each institution to decide to pursue social media policing, the police cannot overlook the growing trend of social media use. With more time spent on social media, the more affinity an individual and the community have, the more it intertwines with their daily lives. Therefore, the demand for 'policing' to be present in this new space has surfaced, and thus, the police must develop best practices for being present in the social media space.

This article will investigate contemporary policing strategies for maintaining a presence in the emerging social media "space" to understand optimal practices for cyber-policing social media. We employ a conceptual research methodology by conducting a comprehensive literature review. This will involve a systematic analysis of literature on crime prevention theories, routine activity theories, and deterrence theories, and an examination of their relevance to the cyber environment. This systematic approach based on literature allows for a comprehensive examination by validating theories and implications of the practice of policing cyberspace without the requirement of empirical research. As a result, we can comprehend the adaptability of conventional crime and policing theories to the the digital realm environment, thereby revealing the potential and constraints of the present cyber-policing methods. This paper will begin by outlining the problem the police face in generating presence in an abstract virtual environment, then it will examine cyberspace enforcement through police cyber-presence, and lastly attempt to negotiate the best practices for police in delivering cyber-presence. This paper will examine the challenges encountered by law enforcement agencies when attempting to establish their presence in a virtual realm with the aim of enforcing the virtual settings. In each section, we addressed these difficulties by proposing effective techniques for cyber-policing. Apart from offering theoretical understanding of virtual-policing, the aim of this research is to focus on offering practical recommendations.

METHODOLOGY

This article employs a conceptual research approach grounded in an extensive literature review to explore the challenges and strategies of policing in cyberspace. The methodology involves systematically analysing existing literature on crime prevention theories, routine activity theory, deterrence theory, and rational choice theory as they pertain to both physical and cyber environments. Key academic texts, journal articles, and authoritative sources were selected to provide a comprehensive understanding of how police presence has traditionally been conceptualized and how these concepts are evolving in the digital age. This literature-based approach allows for a thorough examination of the theoretical underpinnings and practical implications of cyber policing without the need for empirical data collection. Sources were chosen based on their relevance, recency, and contribution to the topic. The review process involved identifying recurring themes, gaps, and emerging trends in the literature, which were then synthesized to construct a coherent narrative about the current state and future directions of cyber policing. By critically engaging with the literature, this journal aims to provide a nuanced understanding of how traditional policing theories can be adapted to the cyberspace context, highlighting both the potential and the limitations of current approaches. This methodology ensures a comprehensive and reflective analysis of the complex dynamics involved in policing the digital world.

While this study employs a purely conceptual approach grounded in an extensive literature review, it is important to acknowledge its inherent limitations. A conceptual framework, while robust in theoretical analysis, lacks empirical data that could provide concrete evidence and validation of the proposed strategies. This limitation is mitigated by relying on a diverse range of authoritative sources, including recent studies, academic texts, and reports from credible institutions, ensuring that the analysis is comprehensive and well-supported. Additionally, by synthesizing findings from multiple sources, this approach offers a holistic view of the challenges and opportunities in cyber-policing, which might not be captured through empirical studies alone. Future research can build on this conceptual foundation by incorporating empirical data to test and refine the proposed strategies, thereby enhancing the practical applicability and effectiveness of cyber-policing methods in the ever-evolving digital landscape.

RESULT AND DISCUSSION

Traditionally, law enforcement preserves public order and deters crime in the physical realm using tangible symbols such as uniforms, badges, and patrol cars to represent authority. These tangible symbols, coupled with direct physical interactions between police and the people, cultivate collective identities that serve as symbolic affirmations of status, thereby legitimizing the police as an integral component of the social order. However, the conventional concept of police presence and approach is profoundly contested by the distinct and intangible nature of the digital environment (Cook & Whowell, Visibility and the Policing of Public Space, 2011, p. 611). The police have attempted to develop a fundamental presence in cyberspace through the creation of official accounts and the enforcement of cyber laws, however they face various difficulties. Issues such as maintaining credibility, ensuring visibility amidst the vast and fast-paced nature of social media, and managing public perceptions are critical. The effectiveness of these strategies is also influenced by the public's trust in the police, which can be fragile in an online context where misinformation and negative sentiments can spread rapidly. These findings underscore the need for innovative approaches and continuous adaptation to enhance the legitimacy and effectiveness of cyber policing.

1. Bridging Physical and Digital Policing Services

In the physical world, Ericson (1982, p. 3) asserts that the police have established their legitimacy as producers of order by instituting systematic micro-level patterns in everyday encounters with the public. This premise is consistent with Interaction Ritual Theory (IRT), which holds that micro-level, face-to-face interactions between police and the public are fundamental because they indicate social order, participation, assurance, and social cohesion (Bowling et al., 2019). IRT was based on the premise that the physical presence of human actors is a necessary component of effective encounters (Collins, 2004: 19). As a result, visibility becomes a critical component of policing. Members of policing institutions, both professional and informal, wear uniforms, vehicles, badges, and other equipment as symbols to convey various messages and

provoke specific emotions in the people who observe them. Thus, the challenge has become how the police might retain a presence in the abstract realm of the internet, which is devoid of tangible rituals and symbols. Henry (2020) reveals that technologies can facilitate policing rituals and could culminate in the same emotion-producing encounters. These mediated encounters could accomplish this by reproducing the elements of interaction rituals by emulating emotional and reciprocal attention, which is why social media is designed to have an emotional impact on keeping us engaged.

A. Establishing a digital presence using social media

Suppose the emulation of his entity can inhibit an individual's presence on social media in the form of an avatar or social media account. In that case, the most basic way the police can be present on social media is to create their official entity akin to its real-world counterpart in the form of an official social media account. Just as individuals might establish their delegated position in the virtual world, several police agencies have interpreted their online presence differently via official accounts. For instance, Police departments around Indonesia have set up Traffic Management Centre (TMC) social media pages to mimic their real-world counterparts' roles of the Traffic Police Cops in updating traffic conditions (Endarnoto, Pradipta, Nugroho, & Purnama, 2011). Another example is how various Australian police supplement their traditional policing programmes such as Neighbourhood Watch and integrate them into Facebook (Kelly & Finlayson, 2015). The role of the official police account can also extend beyond routine policing by providing information on major current events affecting public safety; as demonstrated by the Manchester Police's success in updating information on the 2011 England Riot in order to keep their citizen safe from the ongoing riot (Procter, Crump, Karstedt, Voss, & Cantijoch, 2013) and the Queensland Police Service's success in managing public information for disaster management during the 2011 Queensland Flood (Ehnis & Bunker, 2012). These techniques of defining a social media presence are the most practical approach for the police to be 'visibly' present on social media. As they use the media as a 'medium' of appearing, they construct a space where users can engage with the police the way they usually do in real life.

Unrestricted distance and unhindered time have made it easier for people to share information in cyberspace. This condition has made social media the most popular and effective way for the police to use their official account. Ralph (2022, p. 813) noticed that police content and information shared on social media are believed to be accurate and trustworthy. This is due to the public's confidence in the police, who are known for having a profound comprehension of law enforcement, crime, and disorder, as well as for providing accurate information, as opposed to the contradictory nature of rumour, fake news, and urban myths on social media. The core concept of using an official police account as a platform for information sharing is that better-informed citizens may contribute to public safety by taking proper precautions and avoiding hazardous situations.

Because reaching citizens through police communications is critical to achieving these objectives, this aim will be accomplished only if audiences are reached. However, due to the limitless space available on social media, simply being present does not equate to being 'seen'. While some research has been conducted on the number of followers and reach of official police accounts (Crump, 2011), one cannot presume that followers read all messages. Additionally, the followers of police accounts represent only a fraction of the jurisdiction's population, casting doubt on the effectiveness of using social media accounts for information exchange. Which includes web addresses and hashtags increases the likelihood of transmission, and social media platforms utilise algorithms to organise content based on its frequency of engagement or popularity rather than its substance. As a result, popular content is rendered far more visible than average. Police accounts have a reputation for being typical, uninteresting, and consisting of trivial information. This is because most police officers operate social media in a manner consistent with their real-world stereotype of 'police interaction' distinguished by a formal and distant tone (Bullock, 2018a). The police will need to devise a strategy to become visible in an already congested social media landscape.

Police accounts that are merely ‘appearing’ by conducting information sharing might not have the same form of legitimacy of the police as physical appearance. Whilst the uniform conveys authority and reverence in face-to-face contacts, online encounters are legitimised by expectations of more democratic and “peer to peer” engagement (Goldsmith, 2010). The primary purpose of social media has been to connect with and engage the public; unfortunately, most police accounts have had pretty limited two-way communication (Crump, 2011, p. 23).

Engaging public queries via the official account may eventually supplant the more traditional technique of visiting a police station for officer assistance. When both on- and offline policing produce the same emotion-producing experiences, the public will increasingly accept the police account as a legitimate reflection of real-world policing.

The delegation of police presence in virtual space can only be felt to a certain extent if the police are able to replicate real-world emotion-producing experiences. Police accounts in the virtual world have been deemed “banal” failing to attract a broad audience and unable to be viewed as the police's official representation on social media. Ralph (2022, p. 815) argued that this "banality" of online police information could be overcome by humanising it. This entailed demonstrating police authority in a less authoritative manner through a softer approach, which is bolstered by informal modes of communication. One proven method was done by the New South Wales Police's so-called "meme strategy"; using this strategy, they have transcended the limitation of emotionally charged encounters by incorporating memes or jokes that are pertinent to the audience's lives. While police have used comedy to increase legitimacy, people felt that it also helped police speak about policing subjects and explain police conduct in a more casual, 'humane' manner (Wood, 2020).

We recognize that humor is essential for fostering participation and the police must use discernment in its application, though being adaptable pertains not just to the style of demeanor employed but also to the approach adopted on different platforms. Social media is a very dynamic and turbulent domain in creating and influencing the public discourse on social issues. The narratives that emerge on each social media site frequently differ from one another, often in paradoxical ways. For instance, in the context of disposition and agenda-setting amid the information surge during the COVID-19 pandemic, Bachtiar et al. (2022) revealed that Facebook and Instagram demonstrated a strong positive correlation with government efforts to mitigate the spread of the pandemic, whereas Twitter exhibited a contrasting result. Consequently, the police must adapt and adjust to the characteristics of the diverse online community when conducting virtual policing, as an adaptable strategy to the distinct characteristics of each social media platform will enhance the police’s effectiveness in preserving public order and security in the digital realm.

In order to conduct an effective social media presence, both using an official account and by virtual enforcement; Khan (2018) addressed that sufficient funding needs to be available to support the necessary infrastructure and ensure enough staff have the skills needed to manage social media. With how very constraining the police are with their budget; as a result, training and maintaining a specialist team of trained social media team might not just be plausible for some police departments. Many innovations have tried to resolve budget and personnel limitations in maintaining a social media presence, like the online chatbot system. Gupta et al. (2021) has demonstrated how the use of chatbot could provide an easy-to-use environment where a user can register a complaint and receive police services. The chatbot system provides a more significant benefit by including the complaint in an extensive data system and processing it using data analysis to generate a predictive trend of crime. Cerulo (2011) proposed that sophisticated artificial intelligence and machine learning could enable chatbots to replicate the sensory experiences that characterize real-world police-community contacts, hence facilitating authentic social encounters.

B. Strengthening the legitimacy of virtual-policing

The established approach of the police presence in the abstract domain of social media has been emulated through an official police account and virtual enforcement. The execution of these practices has encountered numerous problems, raising questions about their reliability and legitimacy in the public's perception. The first concern is the credibility of the information being disseminated, followed by the 'banality' or lack of connection with the public, and finally, the ethical concern of covertly enforcing cyberspace. Khan (2018, p. 68) further emphasised the importance of having appropriate resources to support any new policy implementation to ensure its effectiveness. According to Bottoms & Tankebe (2012), residents develop their ideas of police legitimacy on social media in accordance with the police's role and function in the physical world. The police can only be considered legitimate if the information or conditions they publish correspond to those of their real counterparts. Police institutions that appear differently online and offline can be seen as deceptive and eventually illegitimate. As a result, police agencies cannot disregard the role of physical policing in establishing police legitimacy online (Ralph,

2022, p. 816). To preserve legitimacy, the physical and virtual worlds of policing must be inextricably linked; what occurs to the police in the physical world influences the police image in the virtual world, and vice versa. By this premise, if the police choose to be present in the virtual 'space' of social media, the delegation of appearing in the virtual space effectively becomes an inseparable image from policing as a whole.

A successful example of establishing credibility and trust through social media is the Singapore Police Force, which has leveraged social media to combat misinformation and provide accurate information swiftly, thereby building public trust and credibility (Bullock, 2018b). Proactive, transparent communication can enhance the police's online presence and trustworthiness. Yet, there is also the risk of public skepticism towards police communications on social media, especially in regions with a history of strained police-community relations. To address these concerns, police departments must commit to impartiality, ensuring that all communications are fact-based and transparent. Establishing independent oversight committees can also help monitor and maintain the credibility of police social media activities, ensuring they remain trustworthy and unbiased.

The defining nature of credibility on social media is impartial and apolitical, as a result, police accounts can only be considered a reliable source of information if they reflect non-partisan aspects of policing (Bradford & Quinton, 2014). To achieve legitimacy in cyberspace, the police department must first be non-political because if policing is perceived as partisan, universal trust in the police is improbable (Goldsmith, 2005, p. 456). Even though the police endeavour to present all information as impartial, they nonetheless tend to convey biased information about themselves by avoiding disclosing critical internal assessments. This is attributed to his findings that when the police publicised cases that proved they had tackled crime, legitimacy was marginally reinforced since they offered reassurance to the public (Grimmelikhuijsen & Meijer, 2015). In contrast, when officers tweeted negative messages about their performance, the public perceived the police as less effective (de Fine Licht, 2011). Consequently, the general public is growing increasingly critical, Greer and McLaughlin (2010) revealed that the influx of information from citizen journalism will weaken the “official information” provided by police, who have previously held a relatively undisputed position at the top of the “hierarchy of credibility”. Therefore, information released by the police online alone is insufficient and must be supplemented and substantiated by the information shared among the people (De Blasio & Selva, 2021).

C. Enhancing police presence by integrating digital services

Apart from to their presence on social media, the police can enhance their relevance by providing real-world services online to address the challenges of the digital age as well as traditional societal issues. Services include digital driving licenses, electronic criminal records, traffic fines, and information regarding traffic. The Indonesian National Police have progressively adopted this strategy in response to Industry 5.0, which reflects the growing need for digital-based services, as per the modernization agenda of Chief of INP at that time, Police General Tito Karnavian (Batilmurik, Noermijanti, Sudiro, & Rohman, 2019). Although its development had to face numerous challenges, including the tendency for ego-sectoral behavior, wherein each division autonomously creates its own applications and systems without holistic integration. Lufpi et al. (2023) studied the applications utilized by any one Police Department in Indonesia to align with modernization initiatives, identifying a grand total of 71 distinct applications employed by officers, each associated with separate administrators and developers. This does not consider the "dead" applications that become obsolete due to new systems or new regional police chiefs who are reluctant to continue their predecessors' innovations.

According to the study by Lufpi et al. (2023), the primary issue stemming from this ego-sectoral approach is the absence of data integration within divisions, resulting in inefficiencies in service delivery. Independent apps necessitate the public to engage in several repetitious procedures when utilizing different police services, leading to increased operational expenses and extended service durations. Moreover, data security is prone to vulnerabilities, as each division manages data independently without standardized security protocols. This heightens the risk of data breaches and cyberattacks, thereby undermining public trust in the security of their information within the police system. In 2022, the INP developed an integrated Super App that consolidates all previously separate services from various divisions and jurisdictions into a single application, enhancing functionality and addressing the identified issues. This strategy has

established a comprehensive police service application, backed by a user manual and bolstered by risk management and information security measures. Furthermore, the use of this integrated national police strategy has demonstrated an enhancement in personnel engagement and training to facilitate the effective implementation of technology (Jayamuna, 2023).

This unification enables the Police to generate extensive data sets that facilitate swift analysis of cyber risks, online criminal activities, and individuals' conduct in the digital realm. The police can process information in real time, anticipate crime patterns, and react more swiftly to cyber occurrences. This enhances the Police's standing in the digital realm, enabling them to contend with technology advancements while delivering swifter, more precise, and more proactive services to the public. As Williams et al. (2013) shown, machine learning could potentially be used to automate cyber-enforcement processes by assisting dataveillance in analysing online trends. The use of AI-driven chatbots by the Singapore Police Force has streamlined complaint handling and enhanced public service efficiency. Such established methods of integrating artificial intelligence into the process of social media policing had already occurred transpired more than a decade ago; consequently, the future may hold a much more sophisticated method of harnessing the resources in the ever-expanding digital space. Resource intensification has also been seen in the effort to enhance police services in cyberspace. To improve policing services via digital presence and law enforcement on September 20, 2024. The Chief of the Indonesian National Police launched Cybercrime Directorates in eight Provincial Police Departments. The creation of these eight Cyber Directorates illustrates the INP's commitment to improving services at both the National Police Headquarters and Regional Police levels, in reaction to the increasing prevalence of cybercrime in Indonesia.

2. Enforcing the Cyberspace in the Fight Against Cybercrime

Social media's influence is defined by social interactions and the rapid diffusion of information, which are helped by the new environment devoid of physical barriers. However, this enhanced connectivity also promotes a variety of behaviours that may be distressing to another individual and even allows for the existence of crime in this new environment (Clough, 2010, p. 417). The newly developed environment of cyberspace has enabled the development of entirely new forms of activities that are essentially free of traditional and terrestrial limits. As a result, cybercrime and disorder differ significantly from their real-world counterparts; they are more difficult to detect, carry less fear of repercussions due to their anonymity, and can propagate the intended message quickly and inexpensively due. Yar & Steinmetz (2019) provide a comprehensive list of social media misconducts, including but not limited to: sexual harassment, unlawful judgement, invasion of privacy, violation of legal obligations, child pornography, cyberbullying, the spread of hoaxes and hate speech, and even something as massive as an instrument of political uprising.

Individuals might suffer harm due to these activities, including increased levels of emotional and social troubles, physical pain, and difficulty sleeping as a result of cyberbullying and harassing experiences. At the same time, the spread of political attacks on social media has the potential to destabilise a nation, where nation-states pioneered the use of propaganda and fake news for several damaging and immoral purposes (Yar & Steinmetz, 2019, p. 84). Clough (2010) has provided an extensive list of how those various cybercrimes and irregularities in social media have been regulated by legislation enacted by nations worldwide according to their jurisdiction. However, it will not be beneficial if these acts are only policed by a regulative measure where the harms of the action have already taken place. Clough (2010) provides an exhaustive overview of the many forms of legislation enacted by governments worldwide to punish and deter cybercrime and irregularities in social media under their respective jurisdictions. However, it will not be beneficial if these misconducts are only policed through a regulatory mechanism after the resulting harms have occurred. To prevent these misconducts in the first place, the police have implemented various policing techniques to ensure that they are present online as a capable guardian.

A. Application of Routine Activity Theory on Cybercrime

People strive to obey the law when they are in the presence of the police; their presence serves as a symbol that the police are in control, and so diminishes the probability of crime (Doyle, Frogner, Andershed, & Andershed, 2016, p. 21). Cohen & Felson (1979) theorised that criminal activity transpires with the convergence of a motivated offender, a suitable target and the absence of a capable guardian. Henson (2020) developed the adaption of this criminological theory to better understand cybercrime inside this unique virtual framework. This adaptation is

derived on the Theory of Lifestyle Exposure proposed by Hindelang et al. (1978) which claims that victims of crimes are frequently associated with their lifestyles and daily routines. Individuals who traverse dimly illuminated streets daily are more vulnerable to robberies, whereas those residing in lavish properties are more appealing targets for burglary. This idea is then adapted where an individual's online lifestyle or behaviors affect their susceptibility to criminal exploitation in the realm of cybercrime. As a result, individuals who often disclose personal information, such email addresses, phone numbers, or other identifiable data, face a higher chance of being victims of cybercrime. Similarly, individuals with heightened online engagement or exposure are more vulnerable to being targeted by perpetrators, rendering them a more appealing target.

Furthermore, an important aspect in conceptualizing cybercrime is the absence of a physical interaction between the victim and the offender, as opposed to the traditional crime theories. Nonetheless, A motivated offender and the suitable victim does not need to occupy the same time and location, all they need to inhabit is the same "virtual" environment (Reyns, 2013). For example, in a phishing attack, the offender transmits an email or message that appears authentic to the victim in order to acquire personal information, such login credentials or credit card details. Here we see that although the victim and offender do not interact directly, they make use of the same media or platform, like email or direct message. Consequently, using the same media will bring a potential individual closer to a motivated offender and so raise his likelihood of being a victim of cybercrime. This implies that certain media are more vulnerable to cybercrime than others. Visiting dangerous websites, such as illegal streaming platforms, pornography sites, or dark web forums, increases an individual's susceptibility to a virus or online fraud. Though not only harmful websites are the medium, there are several elements determining whether a platform is more vunurable. Including the education of the users, the oversight of the network's developers, and the purpose of the network itself (banking, information sharing, etc.).

The final piece of the Routine Activity Theory is the presence of a capable guardian, which denotes the existence of factors that can deter criminal activity, including police, surveillance cameras, or the proximity of individuals that could be a witness to a crime. In the realm of cybercrime, capable guardian serves as a means of digital defense that can thwart criminal activities. This cyber adaptation of the theory suggests that in cyberspace, temporal and physical constraints no longer impede criminals from reaching a suitable targeted. The figure below illustrates Henson's (2020) adaptation of Routine Activity Theory (RAT) from physical crime to cybercrime, highlighting the revision of Cybercrime RAT theory to focus on the frequent virtual interactions of appealing targets occurring on shared networks lacking effective online guardianship.

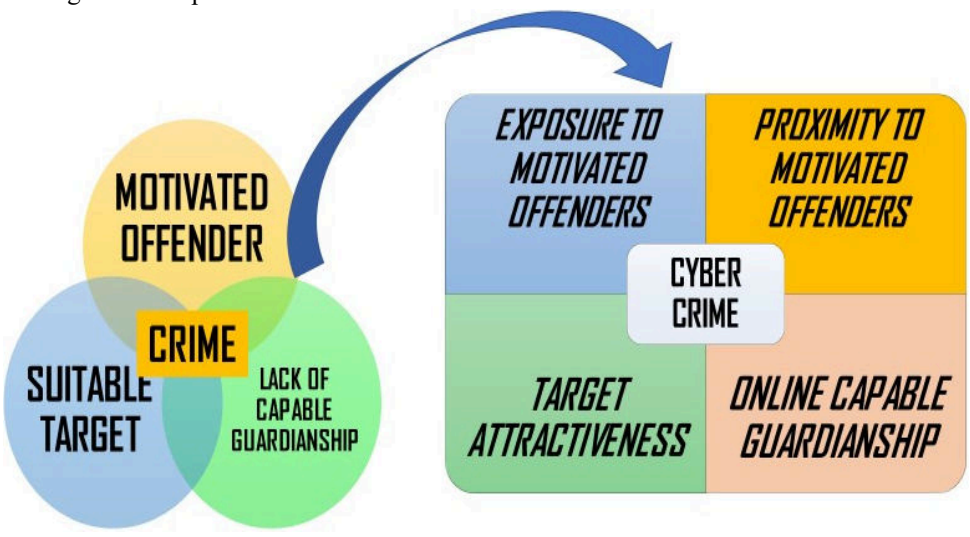

Image 1. Cybercrime Routine Activities Theory (Henson, 2020)

B. Cyber patrol as an online capable guardian

A capable guardian in cyberspace comprises many security protocols designed to safeguard against cyber attacks, including the use of secure passwords, firewalls, antivirus software, and personal precautions such avoiding the indiscriminate sharing of personal information. As individuals increasingly dedicate substantial portions of their lives to the internet, everyday life becomes increasingly intertwined with living online. Consequently, the police's mandate to protect and serve is now required not only in the physical realm but also in the digital domain as a capable guardian (Reynald, 2019). The Indonesian National Police is one example, having launched the "Virtual Police" program, in which officers from the Cybercrime division exercise "cyber patrols" in search of content that breaches the law (i.e. contains hate speech or hoax). The findings will be transmitted to the command centre for legal and linguist opinion from certified experts. If the content breaches the regulation, the virtual police will issue a notification to the user that the content must be removed. If the user does not comply, the user will be requested for clarification and possibly a police investigation (Prabandari, Cahyaningtyas, & Wibawa, 2021). The 'virtual police' have also obtained access to users' personal data in order to be able to impose real-world consequences on people who violate social media regulations, circumventing one of the primary motives for conducting crimes online, anonymity.

The existence of 'virtual police' on social media seeks to replicate Jeremy Bentham's panopticon model, characterized by a central tower overseeing its surrounding prison cells. Due to the panopticon's structural design, inmates at Bentham's prison are constantly aware of the towering silhouette of the central tower; they are conscious of are being spied on but are uncertain of when the detention officers are conducting surveillance (Foucault, 1977, p. 201). Panopticon's philosophy of ensuring visibility has evolved into real-world mechanisms such as CCTV, in which authority is apparent but unverifiable (Foucault, 1977, p. 201). When users are aware that their activities are being 'monitored' by an entity charged with enforcing the law, a mode of social control emerges due to the deterring effect of the concern that the content they post online may break the law (Kim, 2004).

Despite the benefits it offers, the Virtual Police program has encountered criticism about privacy concerns, freedom of expression, and alleged overreach. The presence of virtual police has the potential to provoke discontent among social media users due to the presence in which police monitoring user activity is known. Social media's structural networks had generated communities in areas where users with similar interests or backgrounds congregate, ultimately forming a 'cyber-neighbourhood'. Hinkle and Weisburd (2008) demonstrated that the presence of police results in increased perceptions of insecurity as a result of the view that their 'space' is judged as unsafe. In real-life policing of spaces, widespread surveillance, monitoring, stopping, searching, prosecuting, and investigating members of communities has resulted in the coining of the phrase suspect community (Breen-Smyth, 2014). Casting communities as 'suspect communities' has the potential to generate anxiety and a sense of vulnerability, resulting in long-term dissent with the government and police institutions (Choudhury & Helen, 2011). Such apprehensions are justified, as exemplified by the 2021 event in Solo, where an individual was arrested over a social media remark considered indecent (KOMPAS.com, 2021). Thus, the initiative, while presented as preventive and educative, conflated pre-emptive measures with punitive enforcement, underscoring its potential to suppress legitimate expression. The presence of virtual policing in cyber-neighbourhoods (i.e. the extensive operations of policing hate speech and the spread of false news on social media by opposing activists of a political contest) may result in the formation of suspect cyber-communities with ramifications for their physical user counterparts. As a result, critics contend that expanding law enforcement into personal digital domains jeopardizes the trust between users and authorities.

C. Cybercrime Investigation

The police play a significant role in cybercrime investigations. Specialized units, such as cybercrime divisions within various police agencies, enable law enforcement to monitor, identify, and apprehend cybercriminals. In this framework, the police serve as guardians by both preventing crime and enforcing the law against violators. This encompasses the examination of hacking, identity theft, malware assaults, and several other offenses. To effectively combat cybercrime, law enforcement must receive specialized training and utilize advanced tools. The

growth of technical expertise, such as digital forensics, equips law enforcement to analyze compromised devices, retrieve damaged or encrypted data, and monitor criminal activities online. The primary challenge to virtual enforcement is the jurisdictional variance between social media users. Cyberspace shares the exact perplexing nature of policing in a global world that negates police jurisdictions. Indeed, the notion of policing in cyberspace faces enormous obstacles due to the Internet's worldwide reach.

Police can also work with tech companies and the business sector to make cybersecurity better. This is part of an active prevention strategy by working internet service providers (ISPs) to keep an eye on any strange actions that could be signs of an ongoing cyberattack and take quick steps to stop the attack. Furthermore, the police could form contractual agreements with financial institutions, such as the Internal Revenue Service (IRS) in the United States and the Financial Transaction Reports and Analysis Center (PPATK) in Indonesia, to monitor suspicious transactions and swiftly address cyber threats, thereby deterring individuals from engaging in criminal activities due to the heightened probability of apprehension. In addition, the police could collaborate with banks to improve efforts to deter cybercrime such as online fraud or carding by promptly blocking a suspected fraudulent account to discourage the reward received from online fraud. Finally, law enforcement ought to work with social media and e-commerce companies to monitor and eliminate dubious content or accounts, including fraudulent merchant and phishing scams prevalent on these platforms. This concept is mostly embodied in the Patroli Siber strategy (different from the previously mentioned cyber patrols) of the Indonesian National Police. Patroli Siber is a platform where police from all over the jurisdiction, as well as ordinary citizens, can report malicious websites, social media accounts, or bank accounts that they think are in violation of the law. The Directorate of Cybercrime would then work with internet service providers, social media and e-commerce platforms, banks, and other financial institutions to block the suspect and even put them under criminal investigation (Mahkamah, 2023).

D. Dataveillance as a framework for crime prevention

Social media have prompted individuals to transmit information swiftly across the widely used internet networks. Users can upload content in many formats and share it instantaneously with their entire social connection (Giordano, Spezzano, Sunarsa, & Vinci, 2015). These connections established through user involvement have resulted in an increase in monitoring of daily life; users are prepared to reveal personal information, making their personal lives accessible in ways that have serious ramifications. Mosley Jr. (2012) revealed that insurance firms used social media to gather evidence of fraud, while Lieberman et al. (2013) reported that 59% of police departments use social media data to gather information for use as evidence and monitoring of a suspect. This strategy of policing is referred to as 'Dataveillance,' which is the systematic use of personal data systems to investigate or monitor the actions or communications of one or more individuals (Clarke, 1994)

Policing social media platforms while deploying data surveillance is analogous to the deployment of covert officers. Officers can transform from a visible presence to an anonymous 'user' scouring online, effectively disappearing from public view. Dataveillance can then obtain private and comprehensive information about targeted individuals who are unaware they are being monitored or assisting in investigations. Police officers can quickly gather evidence by simulating how other users access material on the site. This is because a significant amount of information is not secured by privacy settings; any officer may log on and search for evidence; contact information, images, friend lists, and wall posts are technically accessible to all users. Dataveillance does not limit monitoring individuals on social media; the police then have known to utilise social media analytics to use 'cyber-neighbourhoods' present in the social media space to monitor tensions for hate crime and unrest (Williams, et al., 2013). These data are extracted from social media networks in forum involvement, hashtag conventions, and even the geolocation of posts in predicting offline social trends.

Compared to traditional physical or electronic surveillance, dataveillance is inexpensive and continues to become more affordable as information technology advances. However, it is also inevitable that this ease of information sharing will result in an 'information overflow' situation. The massive amount of data generated in social media in such a short period makes it challenging to analyse meaningful datasets, and the interdependence between online expression and offline action is still primarily contested (Williams, et al., 2013). As a result, data such as personal information and rumours on social media networks cannot be used standalone and must

be triangulated with other data sources to produce accurate intelligence. Though, these two methods of police enforcement on social media have created ethical problems due to the ease with which the police can obtain private information, which is illustrated by the asymmetrical relationship between the public and the police on social media. Various legislation, including the United Kingdom's Regulation of Investigatory Powers Act (RIPA) 2000, have created parameters for the police in conducting covert operations (Loftus, Goold, & Mac Giollabhui, 2016). However, no guidelines have been developed concerning the authorisation of anyone, let alone a formal government institution, from exploiting online data for surveillance purposes. Even more concerning is the ethical issue of information gathering in virtual enforcement. The police essentially have access to the real-world information of targets, even though the information is concealed by anonymity and never consented to by the user.

Even though virtual enforcement occurs not in the physical world, it could bring as much consequences to police legitimacy offline. The ability to utilize technology for dataveillance and virtual enforcement is the core component of cyber policing. Thus, the police online also have the authority to exert power and limit the freedom of individuals on the internet, similar to the physical realm. Given the tendency for authority to be misappropriated, it necessitates comprehensive regulation and ethical training in the exercise of power online. As a result, the absence of regulation in conducting dataveillance will need to be addressed by police leadership and the nation's lawmaker; this will ensure the police are able to conduct a legitimised covert social media operation. Casanovas (2017) discusses in detail how accountability, subject access, and consent are central to current European legislation and the General Data Protection Reform package (GDRP). The individual is expected to retain control over the gathered personal data. Generally, informational rights are referred to as ARCO rights (access, rectification, cancellation, and objection). As a result, police activities must adhere to regional, national, and EU legislation. However, modern crime has a transnational, expanded dimension; as a result, criminal data and information subject to dataveillance might not even be stored, handled, or used only in Europe. Therefore, legislators and police leaders must collaborate to discuss the nature of conducting dataveillance on a global scale in order to avoid provoking consent from their people, not only on a national level but also on an international level, as policing and data ownership are no longer geographically limited.

Along with comprehensive and robust legislation, the government neet to address the underlying issue of human and financial resources available so that these social media innovations can be utilised effectively. The complexity and resource-intensiveness of complying with strict data protection regulations, can be challenging for smaller police departments or National Police from smaller nations. Additionally, there might be concerns about the balance between surveillance for security purposes and respecting individual privacy. Thus, governments should invest in training and resources to ensure the Police can comply with data protection laws. Moreover, establishing clear guidelines and oversight mechanisms can help balance security needs with privacy rights, ensuring ethical and effective cyber-policing practices.

E. Community policing the cyber community

Manpower and resources are the most prominent issues facing police globally; low police to people ratio observed in most counties makes it impossible to maintain a continuous police presence over the entire population (Baughman, 2021). This challenge becomes even more pronounced in cyberspace, where police institutions, represented only by their Cyber and Public Relations Divisions, have to contend against the vast and complex network of netizens. As a result, the police must ensure that the populace obeys legal regulations voluntarily, rather than only because the police are monitoring their activities online. The goal of obtaining legal compliance is a complex issue embedded in the foundational principles of community policing (Fine, 2021). In light of this, it is quite clear that the police force ought to incorporate the concepts of community policing into the realm of internet as well. However, the discussion persists over how the notion of physical community might be transformed into an invisible spectacle.

Akbar & Nita (2002) identify a unique concept by examining the role of police intelligence, a unit generally linked to covert operations, in community policing. This expands the notion of community policing beyond the visibility of uniformed officers, indicating that an invisible police presence can also participate in community policing initiatives. According to their research, community policing can be done in a way that can't be seen or touched by talking to people or groups and sharing information with them all the time, even if they don't know what

their part is. In addition, the police give these individuals the instruments they need to take the proactive approach that the police desire, which in this case is to be resilient against radicalism. Consequently, cyber police may theoretically assume a comparable function by participating in community-focused initiatives that enhance public safety in the digital realm.

The fundamental approach to preventing online victimization is implementing personal security measures, so enabling users to safeguard themselves. A highly effective method for law enforcement to serve as cyber guardians is by informing the public about cybersecurity threats and protective measures. Rahmat et al. (2022) claimed that police information campaigns on effective cybersecurity measures, such as employing strong passwords, recognizing phishing attempts, avoiding insecure websites, and utilizing security software like antivirus or firewalls, have been demonstrated as an initial successful strategy to combat cybercrime.

As audiences now are 'increasingly choosing, or being asked to be part of the news-making process', social media interactions can assist the police in resolving crimes. Schneider & Trottier (2012) demonstrated the Vancouver Police were able to solicite information from social media by posting footage and pictures during the 1994 Stanley Cup riots. The capacity of the internet will enable individuals to provide meaningful information to police provides the citizen a voice in the judicial process, allowing the citizen to adopt a 'mutuality' attitude toward the authority during this interaction. However, research conducted by Heaselgrave and Simmons (2016) revealed that only a small number of government agencies engage in two-way communication via social media due to a lack of organisational conception of social media usage, limited practitioner competencies in interactive technologies, and the fear of backlash social media administrators face when engaging and dialoguing through official accounts.

Being positioned in a space where no one is physically restricted from observing the interaction between a police account and its audience leads in a power shift away from the authority and toward the audience. Negative comments can encourage individuals with past negative opinions against the police to speak out online against them, making the public's perception appears more negative than the reality (Lee and Chun, 2016: 486). This is because the social judgement theory (Sherif & Hovland, 1961), that individuals' preceding attitudes serve as a reference point for determining whether they would accept or reject others' opinions. Sukarno and Nur (2022) described how strong sentiment about how police handle a case generated a nationwide outrage on social media, prompting other people to share their unpleasant experiences with the police. This presents the police with a significant challenge in controlling their presence in social media. As Bullock (2018a) claimed that police practitioners see a lack of control on social media as a result of negative comments and backlash. As a result, it is necessary for police personnel to gain back the trust of the community by respecting the populace they serve. As such respect enhances public cooperation and raises the likelihood of acquiring information and making the public comply to the messages delivered by the police (RAND Corporation, 2008).

To enhance online community policing, law enforcement can employ social media monitoring techniques to be informed about community concerns and discussions, enabling prompt and appropriate responses to emerging situations. This proactive strategy not only addresses disinformation but also exemplifies the police's dedication to transparency and accountability (Saputra, 2021). Furthermore, as community policing is a two-way partnership, the police should also include stakeholders within virtual communities to enhance understanding of the public's particular needs and concerns. This allows the police to formulate more focused and effective strategies to ensure public safety and legal compliance (Prisgunanto, Lubis, & Sitorus, 2022). The key aspect is establishing an online atmosphere of respect and reciprocal involvement that can enhance police-community ties and augment their overall performance in upholding law and order.

CONCLUSION

This study seeks to explore how fundamental police practices might be adapted to address challenges in cyberspace by examining methods to improve visibility, credibility, and public trust online. This research extends traditional crime prevention theories, including routine activities theory, deterrence theory, and rational choice theory, to cyberspace, emphasizing the necessity of police physical presence in addressing cybercrime and maintaining social order in online communities. This research extends the usage of traditional crime prevention theories to cyberspace, highlighting the necessity of police presence in addressing cybercrime and maintaining social order in online communities. The results of this study establish a robust basis and actionable suggestions for law enforcement agencies to modify their approaches in light of the continuously changing digital environment. Future research should evaluate the proposed principles to enhance their practical implementation, facilitating the enforcement of law in cyberspace while maintaining ethical and legal standards. This analysis explores the proactive strategies implemented to uphold social order and tackle internet criminal activity within the framework of globalization.

REFRENCES

Batilmurik, R. W., Noermijanti, Sudiro, A., & Rohman, F. (2019). Organizational commitment of police officers: A static study technique in Indonesian national police. *Journal of Advanced Research in Dynamical & Control Systems, 11*(2), 1876-1884.

Baughman, S. B. (2021). How Effective Are Police? The Problem of Clearance Rates and Criminal Accountability. *Alabama Law Review, 72*, 48-113.

Beccaria, C. (1986). *An Essay on Crimes and Punishment.* Indianapolis: Hackett Publishing Company.

Beer, D., & Burrows, R. (2007). Sociology and, of and in Web 2.0: Some Initial Considerations. *Sociological Research Online, 12*(5), 67-79.

Bottoms, A., & Tankebe, J. (2012). Criminology: beyond procedural justice: a dialogic approach to legitimacy in criminal justice. *Journal of criminal law & criminology, 102*(1), 119-170.

Bowling, B., Reiner, R., & Sheptycki, J. (2019). *The politics of the police* (5th ed.). Oxford: Oxford University Press.

Bradford, B., & Quinton, P. (2014). Self-Legitimacy, Police Culture and Support for Democratic Policing in an English Constabulary. *British Journal of Criminology, 54*(6), 1023–1046.

Breen-Smyth, M. (2014). Theorising the "suspect community": counterterrorism, security practices and the public imagination. *Critical Studies on Terrorism, 2*, 223-240.

Bullock, K. (2018a). (Re) Presenting "Order" Online: The Construction of Police Presentational Strategies on Social Media. *Policing and Society, 3*, 345-359.

Bullock, K. (2018b). The Police Use of Social Media: Transformation or Normalisation? *Social Policy and Society, 17*(2), 245-258.

Casanovas, P. (2017). Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In M. Taddeo, & L. Glorioso, *Ethics and Policies for Cyber Operations* (pp. 139-167). New York City: Springer.

Cerulo, K. (2011). Social interaction: do non-humans count? *Sociology Compass, 9*, 775-791.

Choudhury, T., & Helen, H. (2011). The Impact of Counter-Terrorism Measures on Muslim Communities. *International Review of Law, Computers & Technology, 25*(3), 151-181.

Clarke, R. (1994). Dataveillance by Governments. *Information Technology & People, 2*, 46-85.

Clarke, R. (1997). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). New York: Harrow and Heston.

Clough, J. (2010). *Principles of cybercrime* (2nd ed.). Cambridge: Cambridge University Press.

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

College of Policing. (2020). *Policing in England and Wales: Future Operating Environment 2040.* College of Policing Report. Retrieved April 2024, 18, from https://whatworks.college.police.uk/About/News/Pages/Policing2040.aspx

Cook, I., & Whowell, M. (2011). Visibility and the Policing of Public Space. *Geography Compass, 5*(8), 610-622.

Cook, I., & Whowell, M. (2011). Visibility and the Policing of Public Space. *Geography Compass, 5*(8), 610-622.

Crump, J. (2011). What Are the Police Doing on Twitter? Social Media, the Police and the Public. *Policy & Internet, 3*(4), 1-27.

Dau, P., Vandeviver, C., Dewinter, M., Witlox, F., & Vander Beken, T. (2021). Policing Directions: a Systematic Review on the Effectiveness of Police Presence. *European Journal On Criminal Policy And Research*.

De Blasio, E., & Selva, D. (2021). Who Is Responsible for Disinformation? European Approaches to Social Platforms' Accountability in the Post-Truth Era. *American Behavioral Scientist, 65*(6).

de Fine Licht, J. (2011). Do We Really Want to Know? The Potentially Negative Effect of Transparency in Decision-Making on Perceived Legitimacy. *Scandinavian Political Studies, 34*(3), 183-201.

Doyle, M., Frogner, L., Andershed, H., & Andershed, A. (2016). Feelings of Safety In The Presence Of the Police, Security Guards, and Police Volunteers. *European Journal On Criminal Policy And Research, 22*(1), 29-40.

Ehnis, C., & Bunker, D. (2012). Social Media in Disaster Response: Queensland Police Service - Public Engagement During the 2011 Floods. *ACIS 2012 Proceedings.*

Endarnoto, S., Pradipta, S., Nugroho, A., & Purnama, J. (2011). Traffic Condition Information Extraction & Visualization from Social Media Twitter for Android Mobile Application. *Proceedings of the 2011 International Conference on Electrical Engineering and Informatics*, (pp. 1-4).

Ericson, R. (1982). *Reproducing order: a study of police patrol work.* Toronto: University of Toronto Press.

Ericson, R., & Haggerty, K. (1997). *Policing the Risk Society.* Toronto: University of Toronto Press.

Fine, A. D. (2021). Legal socialization: Understanding the obligation to obey the law. *Journal of Social Issues, 77*(2), 367-391.

Foucault, M. (1977). *Discipline and punish : the birth of the prison.* New York City: Pantheon Books.

Giordano, A., Spezzano, G., Sunarsa, H., & Vinci, A. (2015). Twitter to integrate human and Smart Objects by a Web of Things architecture. *19th International Conference on Computer Supported Cooperative Work in Design* , (pp. 355-361).

Goldsmith, A. (2005). Police reform and the problem of trust. *Theoretical, 9*(4), 443-470.

Goldsmith, A. (2010). Policing's New Visibility. *The British Journal of Criminology, 50*(5), 914-934.

Greer, C., & McLaughlin, E. (2010). We predict a riot?: public order policing, new media environments and the rise of the citizen journalist. *British Journal of Criminology, 50*(6), 1041-1059.

Grimmelikhuijsen, S., & Meijer, A. (2015). Does Twitter Increase Perceived Police Legitimacy? *Public Administration Review, 75*(4), 598-607.

Gupta, B., Rustagi, P., Sinha, P., & Sroa, R. (2021). Virtual Police Station System with Chat Bot Using FSM. In A. Nagar, D. . In A. Nagar, D. Singh Jat, G. Marin-Raventos, & D. Kumar Mishra, *Intelligent Sustainable Systems* (pp. 229-236). Singapore: Springer Nature.

Hayes, R. (2019). *Cyber Security and the Importance of Continuous Training.* Rockville: SANS Institute.

Heaselgrave, F., & Simmons, P. (2016). Culture, competency and policy: why social media dialogue is limited in Australian local government. *Journal Of Communication Management, 20*(2).

Henry, A. (2020). Interaction rituals and 'police' encounters: new challenges for interactionist police sociology. *Policing And Society, 31*(9), 1066-1080.

Henson, B. (2020). Routine Activities. In T. J. Holt, & A. M. Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 470-473). London: Palgrave Macmillan.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger Publishing Company.

Hinkle, J., & Weisburd, D. (2008). The irony of broken windows policing: A micro-place study of the relationship between disorder, focused police crackdowns and fear of crime. *Journal Of Criminal Justice, 36*(6), 503-512.

Huey, L. (2002). Policing the abstract: Some observations on policing cyberspace. *Canadian Journal Of Criminology, 44*(3), 243-254.

International Association of Chiefs of Police. (2024, May). *Cybercrime*. Retrieved June 1, 2024, from theiacp: https://www.theiacp.org/topics/cybercrime

Jackson, J., & Bradford, B. (2009). Crime, policing and social order: on the expressive nature of public confidence in policing. *British Journal of Criminology, 60*(3), 493-521.

Jayamuna, I. M. (2023). Sistem Pelayanan Kepolisian Melalui Aplikasi Polri Super App di Polda Lampung Sebagai Inovasi Pelayanan Publik. *Jurnal Socia Logica, 2*(2), 1-12.

Kelly, A., & Finlayson, A. (2015). Can Facebook save Neighbourhood Watch? *Police Journal: Theory, Practice And Principles, 88*(1), 65-77.

Khan, G. (2018). *Social Media for Government.* Singapore: Springer Nature.

Kim, M. (2004). Surveillance Technology, Privacy and Social Control. *International Sociology, 19*(2), 193-213.

KOMPAS.com. (2021). *KOMPAS.com*. Retrieved November 17, 2024, from Mengenal Virtual Police: Definisi, Dasar Hukum, hingga Polemiknya: https://nasional.kompas.com/read/2021/03/17/14414171/mengenal-virtual-police-definisi-dasar-hukum-hingga-polemiknya?page=all

Loftus, B., Goold, B., & Mac Giollabhui, S. (2016). From a Visible Spectacle to an Invisible Presence: The Working Culture of Covert Policing. *British Journal Of Criminology, 56*(4), 629-645.

Lufpi, B., Hutapea, G. T., & Suryadi. (2023). Penyatuan Sistem Informasi Kepolisian yang Terintegrasi untuk Mewujudkan Big Data Polri Guna Peningkatan Kualitas Pelayanan Publik. *Jurnal Ilmu Kepolisian, 17*(1), 51-73.

Mahkamah, R. M. (2023). Upaya Direktorat Tindak Pidana Siber Bareskrim Polri Dalam Mengedukasi Masyarakat Tentang Keamanan Siber di Media Sosial. *Doctoral dissertation, Universitas Nasional*.

Mosley Jr., R. (2012). Social Media Analytics: Data Mining Applied to Insurance Twitter Post. *Casualty Actuarial Society E-Forum, 2*, 1-36.

Police Executive Research Forum. (2013). *COMPSTAT: Its Origins, Evolutions, and Future in Law Enforcement Agencies.* Washington D.C.: Bureau of Justice Assistance.

Prabandari, A., Cahyaningtyas, I., & Wibawa, K. (2021). The Role of Indonesia Virtual Police in Countering Hate Speech on Social Media. *The 2nd International Conference on Law, Economic, Governance.* Semarang: European Alliance for Innovation.

Prisgunanto, I., Lubis, R., & Sitorus, T. (2022). Strategi Pencegahan Penyebaran Berita Hoax Terkait dengan Radikalisme dan Terorisme. *Jurnal Ilmu Kepolisian, 16*(2), 111-125.

Procter, R., Crump, J., Karstedt, S., Voss, A., & Cantijoch, M. (2013). Reading the Riots: What Were the Police Doing on Twitter? *Policing and Society, 4*, 413-436.

Rahmat, A. F., Mutiarin, D., Pribadi, U., & Rahmawati, D. E. (2022). Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling Cybercrime? *2021 Proceedings of the International Conference on Public Organization.* Yogyakarta: APSPA Organization.

Ralph, L. (2022). The dynamic nature of police legitimacy on social media. *Policing and Society, 7*, 817-831.

RAND Corporation. (2008). *Community Policing and Crime: The Process and Impact of Problem-Solving in Oakland.* Santa Monica: RAND Corporation.

Reynald, D. M. (2019). Guardianship in the Digital Age. *Criminal Justice Review, 44*(1).

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency, 50*, 216-238.

Saputra, A. F. (2021). One Nation Under Virtual Office: Kontrol Sosial, Aktivisme Viral, dan Patroli Internet: Aktivisme Viral di Era Patroli Siber. *Jentera: Jurnal Hukum, 4*(1), 414-439.

Schneider, C. J., & Trottier, D. (2012). The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing. *BC Studies, 175*.

Sherif, M., & Hovland, C. (1961). *Social judgment: Assimilation and contrast effects in communication and attitude change.* New Haven, CT: Yale University.

Sukarno, M., & Nur, U. (2022). Public Response on Social Media Narration (Case Study: #PercumaLaporPolisi). *The 2nd International Conference on Government Education Management and Tourism* (pp. 1-5). Bandung: Leo Jejaring Ilmu.

Williams, M., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., . . . Sloan, L. (2013). Policing cyber-neighbourhoods: tension monitoring and social media networks. *Policing and Society, 23*(4), 461-481.

Wood, M. (2020). Policing's 'meme strategy': understanding the rise of police social media engagement work. *Current Issues In Criminal Justice, 32*(1), 40-58.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society.* Thousand Oaks: SAGE Publications.