



Original Article

Cyber Patrol Strategy in Preventing Online Gambling by the Sukabumi District Police

Bima Cahya Juliansyah^{1✉}, Chairul Muriman Setyabudi², Suryadi³

^{1,2,3}Universitas Indonesia, Depok, Indonesia

Correspondence Author: bima.c.juliansyah@gmail.com ✉

Abstract:

This research aims to analyze the effectiveness of cyber patrol strategies implemented by the Sukabumi District Police (Polres Sukabumi Kabupaten) in preventing online gambling, a type of cybercrime that continues to grow in line with the increasing use of digital platforms in society. A qualitative approach with case study methodology is applied to explore in depth the planning, organization, implementation, and control of cyber patrols, as well as the coordination between internal police units and external stakeholders such as Kominfo, ISPs, and financial institutions. Research findings indicate that although regulatory frameworks and operational procedures are available, challenges remain, including limited digital forensic capacity, budget constraints, and low public participation in reporting gambling-related activities. SWOT analysis and the application of Situational Crime Prevention (SCP) theory reveal the need for capacity building of personnel, adoption of advanced detection technologies, and expansion of public education campaigns to strengthen community involvement in online crime prevention. This study recommends the formulation of integrated policies that combine cyber patrol operations with digital literacy, law enforcement, and cross-sector collaboration to create a safer digital ecosystem and reduce the prevalence of online gambling in the Sukabumi District jurisdiction.

Keywords: Cyber Patrol; Online Gambling Prevention; Sukabumi District Police; Crime Prevention; Situational Crime Prevention (SCP).

Introduction

The development of internet technology has brought major changes to human life, affecting almost all aspects ranging from communication, education, to the economy. According to the International Telecommunication Union (ITU), in 2024, more than 5.3 billion people, or nearly 67% of the world's population, were connected to the internet. This figure represents a significant increase, with approximately 97 million new users



recorded within a single year—an increase of 1.8% compared to the previous year ([Kemp, 2024](#)). The growing accessibility of the internet has accelerated the flow of information and opened new opportunities for society to interact, learn, and conduct business more efficiently.

The ease of access to information offered by the internet not only enriches knowledge but also creates a more equal distribution of information. Onno W. Purbo defines the internet as a medium that enables communication to run more effectively through the connectivity of devices and digital applications. Internet use now allows people in various regions, including remote areas, to access education, healthcare services, and learning resources such as online courses and digital libraries ([CNBC Indonesia, 2022](#)). This helps reduce the information gap and supports the realization of equitable knowledge distribution.

In Indonesia, internet penetration continues to show an upward trend. Based on data from the Indonesian Internet Service Providers Association (APJII), the number of internet users in 2024 reached 221.5 million people, equivalent to 79.5% of the total population. This figure reflects a 1.4% increase compared to the previous year and has shown stable growth since 2018 ([Haryanto, 2024](#)). These facts demonstrate that the internet has become a basic necessity for Indonesian society, particularly in supporting digital economic activities, communication, and entertainment.

From a demographic perspective, internet users in Indonesia are dominated by younger generations Gen Z accounts for 34.40% and millennials for 30.62% ([Finaka et al., 2024](#)). This condition indicates that the productive-age group constitutes the primary users of the internet, which indirectly influences the patterns of digital behavior within society. With the high participation of younger generations, the internet has the potential to become a medium for shaping character and fostering a healthy digital culture when used wisely.

However, the advancement of internet technology also brings negative impacts, one of which is the rise of cybercrime. According to the National Institute of Standards and Technology (NIST), cyberspace encompasses the entire information technology infrastructure, telecommunications networks, computer systems, and interconnected industrial control systems. Internet-based crimes such as online fraud, hacking, and online gambling pose a real threat to both individual and national security ([Arifiyadi, 2017](#)).

Online gambling is one of the most prevalent and difficult-to-eradicate forms of cybercrime. This activity is carried out through digital platforms offering various types of betting games, often luring users with promises of large profits. The Head of the Indonesian Financial Transaction Reports and Analysis Center (PPATK), Ivan Yudistavandana, revealed that the circulation of online gambling funds in Indonesia throughout 2024 reached IDR 283 trillion, marking a 237.48% increase compared to the previous year ([Paat, 2024](#)). This surge is driven by easy access, small betting amounts, and aggressive marketing strategies employed by gambling operators.

The online gambling phenomenon not only has economic impacts but also creates social and psychological problems. Cases of online gambling addiction leading to severe financial losses, family breakdowns, and even mental health issues have been increasingly reported. Teenagers and low-income groups are among the most vulnerable due to their limited digital literacy and self-control ([Meswari & Ritonga, 2023](#)). This underscores the urgent need for systematic preventive measures.

In October 2024, the public was shocked by a viral case involving TikTokers in Sukabumi Regency who were caught promoting online gambling accounts. According to a report on Merdeka.com ([Lubabah & Bebeby, 2024](#)), Gunawan Sador was named a suspect for allegedly promoting an online gambling site during a live broadcast on TikTok. Police also named AS, who was his partner, as a suspect in the case. The incident occurred on Saturday, October 26, between 13:30 and 16:00, in Kampung Babakan Baru, Bojongkembar Village, Cikembar District, Sukabumi Regency. During the live broadcast, AS acted as the host and received gifts from a TikTok account named @flogitoto1. After receiving the gift, AS thanked the sender and invited viewers to dance. The live broadcast was later re-uploaded by the @flogitoto1 account. Gunawan, as the account owner, did not take any action to stop the promotion of the gambling site.

According to Sukabumi Police Chief, AKBP Samian, the live broadcast clearly advertised and directed viewers to access online gambling sites available on the internet. Based on the investigation, the account had been receiving gifts since October. Gunawan should have stopped the promotional activity but failed to do so. The case began with reports from residents who were disturbed by the activity. Most of the villagers work as farmers and small business owners, and they had reported the matter to the village head and relevant authorities, but their warnings were ignored. A similar activity had previously been conducted in Bogor but was rejected by the residents, which led Gunawan to return to Sukabumi.

Gunawan and AS now face up to 10 years in prison and a maximum fine of IDR 10 billion, in accordance with Article 45 paragraph 3 in conjunction with Article 27 paragraph 2 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, as well as Article 55 paragraph 1 of the Indonesian Criminal Code (KUHP). Evidence seized in the case includes two cell phones used for the live broadcast, a bank account book under Gunawan's name, the clothes worn by AS during the broadcast, a set of speakers, a tripod, the TikTok account, several screenshots of online gambling activities, and money obtained from the crime. All items have been secured as evidence for the legal process.

On Friday night, November 8, 2024, Sador and AS were granted a suspension of detention. Sukabumi Police Criminal Investigation Unit Head, AKP Ali Jupri, revealed that the decision to grant the suspension was in accordance with applicable legal provisions. The legal basis for the suspension refers to Article 31 of the Indonesian Criminal Procedure Code (KUHAP). He also added that the suspension of detention does not have a specific time limit ([Kurniawan, 2024](#)).

National Police Chief, General Listyo Sigit Prabowo, during a working meeting with Commission III of the House of Representatives (DPR-RI) on Monday, November 11, 2024, stated that Gunawan Sador's detention was suspended, and he was appointed as an anti-online gambling ambassador. The police decided to give Gunawan the opportunity to realize his mistake. The National Police Chief stated that for members of the public who do not fully understand the impact of their actions, the police will provide education and make them ambassadors for anti-gambling campaigns. From the Sador case, the police utilized the information to investigate further and uncover the parties behind the online gambling operation. Police successfully arrested other suspects who acted as marketers and sent gifts during Gunawan's live broadcast ([Rosman, 2024](#)).

Efforts to prevent and enforce the law against online gambling crimes have long been carried out, both by the police as law enforcement officers and by government agencies with authority under the law. In addition to enforcement, the police also have

the responsibility to prevent online gambling crimes. This is closely related to the role of the police in maintaining public security and order. In this context, the police act as the front line in combating online gambling practices. Various preventive strategies can be applied to curb the spread of online gambling in Indonesia. Therefore, this paper focuses on the policing process using a preventive approach.

Although the police have implemented various strategies and measures to enforce the law and prevent the spread of online gambling, the results have not yet been optimal. The Minister of Communication and Digital Affairs stated that from October 20, 2024, to April 23, 2025, more than 1.3 million pieces of content related to online gambling have been handled. This content includes approximately 1,192,000 gambling websites and 127,000 pieces of content circulating on social media.

Gambling has long been a societal problem, and technological developments have made it easier to access through the internet. Although gambling is prohibited under Indonesian law, as stated in the Criminal Code and the ITE Law, online gambling remains widespread. The penalties for offenders are severe, but the effectiveness of these legal provisions is still in question.

Existing regulations are not yet entirely clear and consistent. Differences in sanctions between the Criminal Code and the ITE Law create the potential for multiple interpretations in law enforcement. Some articles can even be interpreted as allowing gambling if a permit is obtained. Supporting facilities such as digital forensic experts, advanced technology, and sufficient funding are not yet fully available. As a result, there are still many loopholes that allow the public to access online gambling sites. Public legal awareness remains low. Many people are not even aware that online gambling is prohibited, so they continue to engage in it. Legal outreach and education need to be intensified to encourage greater public compliance with the law. Social values are also not fully aligned with legal norms. Although gambling is viewed negatively, adherence to the law has not yet become a strong habit or cultural norm.

The Government of Indonesia, through Presidential Decree Number 21 of 2024, has established the Online Gambling Eradication Task Force involving various ministries and institutions, including the National Police (Polri), the Ministry of Communication and Information (Kominfo), the National Cyber and Crypto Agency (BSSN), and PPAATK. These efforts are carried out not only through law enforcement but also through website blocking, financial transaction monitoring, and public education. Nevertheless, these initiatives still face challenges, particularly in ensuring sustainable monitoring and addressing the low level of legal awareness among the public.

As the frontline institution in maintaining public security and order, the National Police (Polri) plays a crucial role in preventing the spread of online gambling. One of the steps taken is cyber patrols, which involve active monitoring of cyberspace to detect and take action against illegal activities. However, the effectiveness of cyber patrols still requires strengthened strategies, technological integration, and cross-sectoral collaboration to produce optimal results.

Based on the aforementioned background, this study focuses on analyzing cyber patrol strategies in preventing online gambling crimes, particularly within the jurisdiction of Sukabumi District Police (Polres Sukabumi Kabupaten). By using Management Theory, and Situational Crime Prevention (SCP) this research is expected to provide comprehensive strategic recommendations to create a safer digital environment, improve public digital literacy, and support the realization of public security and order in the digital era.

Methods

This study employs a qualitative approach with a case study methodology to gain an in-depth understanding of cyber patrol strategies in preventing online gambling by the Sukabumi District Police. The qualitative approach was chosen because this research focuses on obtaining a deep comprehension of the phenomenon under investigation rather than merely measuring numbers or variables. The data collected consists of words, narratives, and descriptions, which are then analyzed to discover meanings, patterns, and relationships between phenomena.

This research uses an exploratory research type. Exploratory research aims to explore, understand, and discover preliminary information about a phenomenon or problem that has not been extensively studied in depth.

The data sources consist of both primary and secondary data. Primary data collection techniques include interviews, observations, and questionnaires directed at relevant stakeholders. Meanwhile, secondary data is obtained from existing sources such as official reports, articles, or other relevant documents.

The data collection techniques applied include interviews, observations, and documentation. These techniques assist the researcher in gathering comprehensive information regarding the implementation of cyber patrols and efforts to prevent online gambling. Each technique serves a specific function and provides a different dimension to the data collected, resulting in a more comprehensive analysis. It is essential to include comprehensive details to enable the replication of the work. When a reagent is utilized in the study, it is important to specify the supplier's information when applicable. Any methods that have been previously published should be cited appropriately, with only pertinent modifications being outlined. In the context of epidemiological studies.

Results

Sub 1 Cyber Patrol Strategy in Preventing Online Gambling by the Sukabumi District Police

The cyber patrol strategy in preventing online gambling by the Sukabumi Regency Police should ideally produce optimal results. However, the persistent prevalence of online gambling indicates that there are areas of management that must be further optimized. In *Basic Principles of Management* (2019), George R. Terry, a renowned management expert who developed highly influential management theories in the 1950s, defines management as a process of planning, organizing, directing, and controlling human and material resources to achieve predetermined goals. [\(Terry & Rue, 2019\)](#)

Planning is the process of determining objectives and the steps needed to achieve them. At this stage, managers decide what the organization aims to accomplish and the best ways to achieve those goals. In an interview with the Head of the Tipidter Unit of Sukabumi Regency Police, it was revealed that cyber patrol planning has been carefully prepared, considering that the leadership has issued clear instructions to conduct cyber patrols to prevent online gambling. Tipidter personnel are assembled and given special directions to take follow-up action in online gambling prevention efforts. The unit head plays an active role in providing directions for the steps to be taken moving forward.

Organizing involves structuring resources and tasks so that the plan can be executed effectively. This includes task distribution, defining responsibilities, and arranging organizational structure. The goal is to create a systematic workflow so that objectives can be achieved efficiently.

Cyber patrol management for online gambling prevention by the Sukabumi Regency Police is a process that requires integrated planning, organizing, implementation, and controlling. Referring to George R. Terry's management theory, this process begins with thorough planning, namely setting the main objective of reducing the number of online gambling cases within the jurisdiction of the Sukabumi Regency Police. Planning includes mapping potential threats, identifying platforms and applications used for online gambling, preparing cyber patrol schedules, as well as strategies for legal socialization and digital literacy campaigns for the community. With proper planning, the Tipidter Unit can anticipate the ever-evolving modus operandi of offenders.

The next stage is organizing, which involves structuring resources so that plans can be executed effectively. The Tipidter Unit forms a cyber patrol team consisting of investigators, IT analysts, and public relations personnel, with clear task distribution. Coordination is also carried out with external parties such as the Ministry of Communication and Information Technology, internet service providers, and banking institutions to cut off online gambling transaction channels. A well-structured organization enables rapid response to public reports and findings during cyber patrol operations.

Following that, the implementation stage is carried out by mobilizing all personnel according to plan. Cyber patrols are conducted regularly during peak gambling activity hours, accompanied by legal education and outreach to the public, both through face-to-face activities and digital campaigns on the official social media platforms of Sukabumi Regency Police. Legal enforcement is also carried out firmly against online gambling operators and players to create a deterrent effect. At this stage, leadership motivation and direction play a crucial role in maintaining personnel morale so that prevention targets can be met.

The final stage is controlling, which refers to the supervision of all cyber patrol activities. Regular evaluations are conducted by comparing case data before and after the implementation of cyber patrols. If weaknesses are found, such as a lack of personnel or information leaks, corrective actions are taken, such as revising strategies or strengthening support facilities. This ensures that the prevention program continues to adapt to the increasingly complex dynamics of cybercrime.

In addition to implementing the four management functions, the Tipidter Unit also optimally manages organizational resources. Human resources are placed according to their competencies and are given continuous training to master digital forensics and cyber investigation techniques. Capital resources are used wisely for procuring detection software, server equipment, and community education costs. The methods applied include modern approaches such as Open Source Intelligence (OSINT) and digital profiling to accelerate offender identification. Material resources, including high-performance computer equipment, secure internet networks, and integrated databases, are ensured to be available as needed. Balanced management of these four resources supports effective cyber patrol operations.

Through the comprehensive application of George R. Terry's management functions, cyber patrol management in Sukabumi Regency Police is not merely a routine task but a comprehensive strategy capable of creating a safe digital ecosystem. This approach strengthens public trust and demonstrates that the police can adapt and remain responsive to the growing threats of online crime.

Cyber patrols conducted by the Sukabumi District Police play a crucial role in reducing the opportunity for online gambling crimes by continuously monitoring cyberspace and identifying illegal gambling activities before they spread widely. This aligns with the Rational Choice Theory, which assumes that individuals weigh the risks and benefits before committing a crime. By intensifying cyber patrols and ensuring that perpetrators are swiftly detected and prosecuted, law enforcement increases the perceived risk, thereby deterring potential offenders. (Djamin, 2015)

The application of Social Disorganization Theory can be seen in efforts to foster healthy online communities through public education about the dangers of online gambling and promoting digital literacy. By creating a “cleaner” virtual environment, the police reduce the opportunity for illegal activities to flourish, particularly in communities vulnerable to exploitation.

Through the lens of Strain Theory, cyber patrols help reduce the motivation of individuals who may turn to online gambling due to economic pressure or limited access to legitimate entertainment options. By combining patrol efforts with preventive programs such as community engagement and economic empowerment, the police can help address underlying strains that drive individuals toward crime.

The Social Learning Theory highlights the importance of breaking the cycle of negative influence within online communities where gambling activities are normalized. Cyber patrols, combined with public awareness campaigns, serve to disrupt these networks and replace them with positive role models, discouraging the spread of harmful behavior.

In the context of Social Control Theory, cyber patrols strengthen social oversight in the digital sphere by collaborating with internet service providers, online platforms, and the public to report and block access to illegal gambling websites. This reinforces the presence of “guardianship” and reduces opportunities for rule violations.

The Labeling Theory also plays a role when law enforcement publicly announces the arrests of online gambling perpetrators. This not only serves as a deterrent but also sends a strong message that such activities are considered crimes under the law, thereby influencing societal perceptions.

From an Environmental Approach, cyber patrols are a situational crime prevention strategy that modifies the digital environment by blocking websites, taking down servers, and restricting access to gambling platforms. This reduces the opportunities for offenders to commit crimes.

From a Social Approach, police efforts include collaborating with local communities to raise awareness about the dangers of online gambling, educating youth, and engaging stakeholders to prevent vulnerable groups from becoming involved in illegal activities.

Lastly, from a Criminal Justice Approach, the Sukabumi District Police integrate cyber patrols with law enforcement actions, including investigation, prosecution, and rehabilitation of offenders. This ensures that those caught engaging in online gambling are processed through the justice system, reducing recidivism.

Overall, cyber patrols are an effective blend of primary, secondary, and tertiary prevention strategies. They modify the online environment to make crime more difficult (primary prevention), identify potential offenders early and provide interventions (secondary prevention), and take firm legal action against proven offenders (tertiary prevention).

Situational Crime Prevention (SCP), developed by Ronald V. Clarke, is one of the most effective criminological approaches to crime prevention by modifying situations or environments that enable criminal acts. This principle is relevant for application in the context of online gambling prevention, which is one of the main focuses of the Tipidter Unit's cyber patrol. Using the SCP approach, prevention efforts are not only aimed at prosecuting offenders after the crime occurs but also at reducing opportunities for crime before it happens. (Clarke, 1997)

First, the strategy of increasing offender effort can be implemented by strengthening technical barriers to access online gambling sites. Cyber patrols work with the Ministry of Communication and Information Technology to block domains and applications used by offenders, forcing them to expend more resources to reactivate platforms or find new channels. In addition, the use of automatic detection technology and filtering algorithms helps narrow offenders' room for movement in the digital space.

Second, the aspect of increasing risks for offenders becomes the core of cyber patrols. The active presence of the Tipidter team in monitoring and sweeping online gambling sites creates a deterrent effect. The risk of arrest increases because every suspicious activity, such as unusual financial transactions or the spread of gambling links on social media, can be detected in real time. Swift law enforcement and publicizing case results also strengthen the perception of risk among potential offenders.

Third, the principle of reducing rewards is applied by cutting off financial transaction channels for gambling. Sukabumi Regency Police cooperates with banks and fintech companies to trace gambling-related accounts and immediately freeze them. As potential financial gains decrease, the attractiveness of engaging in gambling diminishes.

Fourth, the strategy of reducing provocations is implemented through education and digital literacy campaigns. The Tipidter Unit conducts outreach to the public regarding the dangers of online gambling, its legal consequences, and how to recognize scams that often accompany gambling activities. This education reduces public interest and the likelihood of being provoked to participate in gambling.

Lastly, the principle of removing excuses is realized by reinforcing legal norms and ethics. Warning messages are displayed on social media, the official police website, and digital campaigns to raise awareness that online gambling is a criminal offense. These efforts reduce offenders' rationalizations, such as viewing online gambling as "harmless entertainment."

Through the implementation of these five SCP principles, Sukabumi Regency Police's cyber patrol can build a more comprehensive prevention system. This approach not only suppresses the incidence of online gambling but also creates a safer digital ecosystem. Collaboration between cyber patrol teams, government agencies, internet service providers, financial institutions, and the public becomes the key to successfully modifying situations so that crime opportunities are minimized.

Thus, integrating SCP theory into cyber patrol practice provides a strong analytical framework and a foundation for evidence-based policing. This step supports the vision of Sukabumi Regency Police to not only be reactive in tackling crime but also proactive in creating a digital environment free from online gambling.

In the context of preventing online gambling, coordination becomes a key element that must be emphasized by the Sukabumi District Police. Clear information delivery, accurate communication, and well-structured task distribution allow all involved units—such as the cyber unit, criminal investigation division, public relations, and community police officers (Bhabinkamtibmas)—to work according to their respective

responsibilities. This aligns with Hasibuan, who states that coordination is the activity of directing, unifying, and organizing all management elements so that organizational goals can be achieved. Without proper coordination, cyber patrol efforts risk being ineffective, as information may not be conveyed properly, investigations may overlap, and the results of enforcement actions may be difficult to measure accurately. ([Hasibuan, 2006](#))

Good coordination also creates alignment of objectives and activities among units, as explained by Handoko. In handling online gambling cases, cyber patrol is not limited to prosecuting offenders but also requires cross-functional collaboration, such as working with the Ministry of Communication and Information (Kominfo) to block illegal websites, conducting legal education for the public, and involving local leaders to raise legal awareness. Through effective coordination, all these efforts can be carried out efficiently and in a targeted manner, making preventive measures more impactful. ([Handoko, 2003](#))

Furthermore, G.R. Terry emphasizes the importance of the right amount, timing, and direction of activities in coordination. This is highly relevant when the Sukabumi District Police determines cyber patrol schedules, adjusts monitoring intensity during high-risk hours, and ensures that every action taken supports the primary goal—cutting off access to online gambling platforms within Sukabumi’s jurisdiction. Without clear timing and direction, patrol activities risk becoming reactive, acting only after public complaints are received, and thus failing to significantly reduce the number of violations through prevention.

In addition, coordination requires a sense of cooperation, healthy rivalry, team spirit, and esprit de corps. In the context of cyber patrol, team members must support one another and share information openly, rather than working in isolation. Healthy competition can be reflected in performance evaluations that encourage each officer to improve the quality of digital investigations. With strong team spirit, the cyber patrol unit can respond more effectively to public reports and quickly take action against accounts or websites promoting online gambling.

Sub 2 SWOT Analysis of Cyber Patrol Strategy by Sukabumi District Police in Preventing Online Gambling.

Cyber Cyber patrols conducted by the Sukabumi District Police are one of the main strategies in preventing cybercrime, particularly online gambling, which is becoming increasingly widespread and threatens public order. These activities do not solely focus on law enforcement but also include prevention, early detection, and public education. This approach aligns with the modern policing paradigm that emphasizes the importance of prevention (prevention-oriented policing) as an effort to reduce opportunities for crime to occur in cyberspace. By utilizing available human resources and technological infrastructure, cyber patrols serve as the frontline in creating a safe digital space. Using SWOT analysis, it is possible to map out internal and external factors that influence the success of this program. This analysis aims to determine the position of the Sukabumi District Police in dealing with digital threats while formulating more targeted strategies. ([Rangkuti, 2018](#))

In terms of strengths, the Sukabumi District Police have personnel assigned to the Tipidter (Special Crimes Unit) who have received technical training related to cybercrime. This competence enables them to effectively detect and analyze online gambling sites or applications. In addition, regulatory support, such as the Electronic

Information and Transactions Law (ITE Law) and national police policies, provide a strong legal foundation for enforcement. The police also have access to the National Police Headquarters data center, which allows faster tracking when criminal indications are found in the digital space.

Another notable strength is the good internal coordination between the Criminal Investigation, Public Relations, and Community Development units. This collaboration allows for the implementation of a holistic strategy that includes prevention, public awareness campaigns, and law enforcement. With regular patrols in cyberspace, a deterrent effect is created that can reduce offenders' intentions to commit illegal acts. This effect is critical in shaping perpetrators' perception of risk, making them think twice before committing a crime.

Nevertheless, there are weaknesses that need to be addressed. One of them is the limited number of personnel skilled in digital forensics, which can delay the resolution of cases requiring in-depth analysis. Budget limitations are also a challenge, especially in updating detection software and conducting continuous training for members. As a result, cyber patrols tend to be reactive, responding only after receiving reports from the public.

Moreover, the absence of a massive digital literacy program in the Sukabumi District means that the community is not fully aware of the risks and negative impacts of online gambling. Low public participation in reporting puts the entire burden of monitoring the digital space on law enforcement officers. This situation can reduce the effectiveness of prevention efforts because surveillance becomes uneven across all layers of society.

From the perspective of opportunities, the Sukabumi District Police can strengthen synergy with various stakeholders. The Ministry of Communication and Information Technology (Kominfo), internet service providers (ISPs), financial institutions, and educational institutions can be strategic partners in cutting off illegal transaction networks while simultaneously educating the public. Technological developments such as artificial intelligence, big data analytics, and OSINT (Open Source Intelligence) also present opportunities to detect gambling activity patterns faster and more accurately.

Another opportunity lies in the growing public awareness of the dangers of online gambling. This can be utilized to encourage public participation in reporting, enabling cyber patrols to operate more proactively. By building a digital community that is aware of cybersecurity, the Sukabumi District Police can establish an early detection system based on community participation.

However, several threats must be anticipated. The modus operandi of online gambling operators is becoming increasingly sophisticated, using encryption, VPNs, and digital payment systems or cryptocurrencies that are difficult to trace. Moreover, servers located overseas complicate law enforcement efforts due to jurisdictional limitations. Another threat is the risk of data breaches and digital identity theft, which can erode public trust in cyberspace security.

Social threats are also a major concern. High unemployment rates and economic pressures can drive some members of society to seek quick income through online gambling. If cyber patrols fail to significantly reduce the number of cases, the legitimacy of the police in the eyes of the public may decline. This could create a negative perception that law enforcement is ineffective in protecting citizens from digital crimes.

Based on the SWOT analysis, the strategy that needs to be implemented is to maximize internal strengths by increasing personnel capacity, strengthening

technological infrastructure, and leveraging external opportunities through cross-sector collaboration. Digital literacy campaigns must be intensified so that the community becomes a partner in online gambling prevention efforts. With well-planned steps, the Sukabumi District Police can create a safer digital ecosystem, reduce online gambling rates, and improve public trust in law enforcement institutions.

Conclusion

Cyber patrols conducted by the Sukabumi District Police represent a comprehensive strategy that integrates modern management functions, crime prevention theories, and SWOT analysis to reduce the prevalence of online gambling in their jurisdiction. Referring to George R. Terry's management theory, the implementation of cyber patrols follows four key functions: planning, organizing, actuating, and controlling. Careful planning involves threat mapping, patrol scheduling, and digital literacy strategies. Organizing ensures a clear division of tasks between investigators, IT analysts, and public relations officers, as well as coordination with the Ministry of Communication and Information Technology (Kominfo), ISPs, and financial institutions. Patrols are carried out regularly and accompanied by legal education campaigns, while control functions ensure continuous evaluation and adaptation to the evolving modus operandi of cybercriminals. The SWOT analysis shows that Sukabumi District Police possess strengths such as trained personnel, strong legal frameworks, and solid internal coordination. However, there are weaknesses including limited digital forensic resources, budget constraints, and low levels of public digital literacy. On the other hand, there are opportunities to leverage advanced technologies (AI, big data, OSINT) and strengthen cross-sectoral partnerships. Meanwhile, threats include increasingly sophisticated criminal methods, foreign-based servers, and socioeconomic factors driving people to gamble.

By integrating Situational Crime Prevention (SCP) principles, cyber patrols increase offenders' efforts and risks, reduce potential rewards, minimize provocations, and eliminate justifications for gambling. These efforts are reinforced through primary prevention (public education and digital literacy campaigns), secondary prevention (early detection and intervention), and tertiary prevention (strict law enforcement and asset seizure). Overall, the cyber patrol program of Sukabumi District Police is not merely a routine activity but a proactive, evidence-based policing strategy capable of creating a safer digital ecosystem, reducing online gambling cases, strengthening social cohesion, and increasing public trust in law enforcement. To achieve optimal results, it is necessary to enhance human resource capacity, upgrade technological infrastructure, and encourage active community participation in reporting and prevention efforts.

Suggestion

The cyber patrol strategy implemented by the Sukabumi District Police has proven effective in reducing cases of online gambling; however, its sustainability requires further strengthening through the enhancement of human resource capacity, the utilization of more advanced technologies, and the provision of adequate budgetary support. Cross-sector collaboration with relevant institutions and internet service providers should be continuously developed, alongside active community participation in monitoring and reporting. Through these measures, the cyber patrol strategy will become more sustainable, adaptive to evolving crime patterns, and capable of enhancing public trust in law enforcement authorities.

References

- Arifiyadi, T. (2017). Dunia siber yang tidak maya. *Hukumonline*. Retrieved September 24, 2025, from <https://www.hukumonline.com/berita/a/dunia-siber-yang-tidak-maya-1t59c88b4e7bae6/>
- Clarke, R. V. (1997). *Situational crime prevention: Successful case studies*. New York: Harrow and Heston.
- CNBC Indonesia. (2022, September 21). Mengenal apa itu internet, sejarah perkembangan & manfaatnya. *CNBC Indonesia*. Retrieved September 24, 2025, from <https://www.cnbcindonesia.com/tech/20220921131159-37-373856/mengenal-apa-itu-internet-sejarah-perkembangan-manfaatnya>
- Djamin, A. (2015). *Manajemen sekuriti di Indonesia: Buku panduan crime and loss prevention* (R. Lihawa, Ed.). Jakarta: Yayasan Pengembangan Kajian Ilmu Kepolisian.
- Finaka, A. W., Nurhanisah, Y., & Syaifullah, A. (2024). 221 juta penduduk Indonesia makin melek sama internet. *Indonesia Baik*. Retrieved September 24, 2025, from <https://indonesiabaik.id/infografis/221-juta-penduduk-indonesia-makin-melek-sama-internet#:~:text=Pengguna Internet Tahun ke Tahun,orang pada periode 2022-2023>
- Handoko, T. T. (2003). *Manajemen sumber daya manusia*. Yogyakarta: BPFE.
- Haryanto, A. T. (2024). APJII: Jumlah pengguna internet Indonesia tembus 221 juta orang. *DetikInet*. Retrieved September 24, 2025, from <https://inet.detik.com/cyberlife/d-7169749/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Hasibuan, S. M. (2006). *Manajemen sumber daya manusia*. Jakarta: Bumi Aksara.
- Kemp, S. (2024). Internet use in 2024. *Datareportal*. Retrieved September 24, 2025, from <https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption>
- Kurniawan, E. (2024, November 11). Gunawan Sadbor Tiktoker Sukabumi bebas penjara, ini alasannya! *Tribunnews*. Retrieved September 24, 2025, from <https://m.tribunnews.com/regional/2024/11/11/gunawan-sadbor-tiktoker-sukabumi-bebas-penjara-ini-alasannya?page=all>
- Lubabah, R. G., & Bebeby, A. (2024). Kronologi Gunawan Sadbor jadi tersangka: Dari aksi joget-joget, berujung terjerat kasus judi online. *Merdeka*. Retrieved September 24, 2025, from <https://www.merdeka.com/peristiwa/kronologi-gunawan-sadbor-jadi-tersangka-dari-aksi-joget-joget-berujung-terjerat-kasus-judi-online-228274-mvk.html?page=2>
- Meswari, A. S., & Ritonga, M. (2023). Dampak dari judi online terhadap masa depan pemuda, Desa Air Buluh Kec. Ipuh Kab. Mukomuko Provinsi Bengkulu. *Jurnal Cakrawala Ilmiah*, 2(5), 2097–2102. <https://doi.org/10.53625/jcijurnalcakrawalailmiah.v2i5.4642>
- Paat, Y. P. (2024). Capai Rp 283 T, PPATK ungkap cara bandar siasati transaksi judi online. *Investor*. Retrieved September 24, 2025, from <https://investor.id/nasional/379253/capai-rp-283-t-ppatk-ungkap-cara-bandar-siasati-transaksi-judi-online>
- Rangkuti, F. (2018). *Analisis SWOT: Teknik membedah kasus bisnis*. Jakarta: Gramedia Pustaka Utama.
- Rosman, A. (2024). Alasan Polri bebaskan Gunawan Sadbor dan angkat jadi duta anti-judi online. *Katadata.co.id*. Retrieved September 24, 2025, from <https://katadata.co.id/berita/nasional/6731c80fe7c56/alasan-polri-bebaskan-gunawan-sadbor-dan-angkat-jadi-duta-anti-judi-online>
- Terry, G. R., & Rue, L. W. (2019). *Dasar-dasar manajemen*. Jakarta: Bumi Aksara.