Journal Of Social And Political Science
Volume 02,No.2 Tahun 2025
https://rumah-jurnal.com/index.php/jsaps/index

Hybrid Terrorism and Organized Crime Networks in the Asia-Pacific Region: Examining the Links between Cybercrime and Violent Extremism

Emmanuel E. Odeh[1]; Desmond O. Onwo [2]; Ikenna M. Ogbuka[3] and Innocent U. Duru[4]
[1]Department of Political Science, Rhema University Nigeria, Aba, Abia State
odeson_son@yahoo.com
[2]Department of Political Science, Caritas University, Amorji-Nike, Enugu
drnnaaonwo@yahoo.com
[3]Department of Political Science, Enugu State University of Science and Technology, Enugu
ogbuka79@gmail.com
[4]Department of Economics, Rhema University Nigeria, Aba, Abia State
uchechukwuduru1@gmail.com
Corresponding Author: Emmanuel Ejike Odeh
odeson_son@yahoo.com
ORCID: 0000000156302575
+2348068437797

Abstract:
Hybrid terrorism and organized crime networks have become serious security threats in the Asia-Pacific region, with cybercrime playing an increasingly prominent role in funding and spreading their violent extremist activities. Long-running illicit activities in the area by organized crime groups include the trafficking of drugs, the smuggling of people, and money laundering. This paper examines the links between cybercrime and violent extremism, highlighting the use of social media and other online platforms by organized crime networks and the radicalization of violent extremism in the Asia-Pacific region. The paper based its theoretical framework on social learning theory, and an ex-post facto research design was adopted, while its methods of data collection were documentary and survey. Content and qualitative analysis were utilized to analyze the data obtained. The extensive use of social media and other online platforms by organized crime networks has been found to be a significant factor in the growing trend of violent extremism in the Asia-Pacific region. It is recommended that governments and law enforcement agencies engage in proactive monitoring and take the necessary measures to combat these hybrid networks.

Keywords: **Asia-Pacific Region, Cybercrime, Hybrid Terrorism, Organized Crime Networks, Violent Extremism and Security Threats**

Introduction

The Asia-Pacific region, covering more than one-third of the earth's surface and home to over half of the worlds' population, has become a major hub for organized crime networks operating across borders (Allwright & Wright-Neville, 2019). The region has also experienced a surge in violent extremism, including the activities of extremist groups such as ISIS, Al-Qaeda, and their affiliates (Leighton, 2020). In many cases, these extremist groups are closely affiliated with organized crime networks, creating a hybrid threat that exploits both conventional and online channels to propagate their activities and fund their operations.

The Asia-Pacific region has long been a hotbed for criminal and terrorist activities, and in recent years, the threat landscape has evolved. With rapid technological advancement and globalization, the world has become more interconnected than ever before, and this has created new opportunities for illicit activities; and criminals and terrorists are turning to hybrid tactics to exploit these developments. Hybrid terrorism refers to the use of terrorist methods in conjunction with the structures and tactics of organized crime networks, resulting in a formidable threat to global security (Leighton, 2020). Likewise, cybercrime and violent extremism have become increasingly intertwined, with extremist groups using online platforms to recruit, radicalize, and communicate with their

followers and also posing a significant threat to global security (Sahin & Hulagu, 2019). In recent years, there has been a growing concern about the links between cybercrime and violent extremism in the Asia-Pacific region. Cybercriminals are also collaborating with extremist groups to distribute propaganda, recruit new members, and execute attacks (Raza, 2018; Tagliarina, 2018).

Hybrid terrorism and organized crime networks have become serious security threats in the Asia-Pacific region, particularly in countries such as Afghanistan, Pakistan, and the Philippines with cybercrime playing an increasingly prominent role in funding and spreading their violent extremist activities (Global Initiative against Transnational Organized Crime, 2021). These groups often work together to achieve their goals, with terrorism providing a source of funding and protection for organized crime and illicit activities, such as drug trafficking, human trafficking, money laundering, smuggling of weapons and counterfeit goods (Rothe, 2017).

The rise of hybrid terrorism and organized crime networks in the region can be attributed to factors such as socioeconomic inequality, political instability, corruption, and weak law enforcement. These factors create an environment that is conducive to the growth and proliferation of these criminal networks. The factors that drive the spread of criminal networks in Southeast Asia are many and inter-related; they include poverty and inequality, rapidly growing populations, corruption, weak or ineffective governance, the trafficking of human beings and other illicit goods, regional conflicts and security challenges. (United Nations Office on Drugs and Crime, 2019). Socioeconomic conditions like poverty, joblessness, and inequality create fertile ground for terrorist organizations to grow and conditions of rampant corruption with impunity also enable extremist groups to thrive in Asia Pacific region (RAND Corporation, 2021). Hybrid criminal-terrorist groups in the region have also benefited from political instability, conflicts, poverty, and corruption (Interpol, 2021).

The convergence of cybercrime and terrorism has given rise to a new form of criminality that is difficult to detect and disrupt (United Nations Office on Drugs and Crime, 2019). Cybercrime has become the preferred method for funding terrorism (their activities) and expanding their operations and hackers are being hired by terrorist groups to facilitate criminal activities such as money laundering, identity theft, and the theft of intellectual property (Europol, 2016; Alvi, 2020). Organized crime in the Asia-Pacific is expanding, becoming more sophisticated and diversifying its activities. This has led to an increase in the activities of hybrid criminal-terrorist groups in the region (Interpol, 2021). At the same time, violent extremist groups have also begun to use cybercrime as a means of communication, propaganda, and recruitment (Enders & Sandler, 2012). The use of the internet and social media by extremist groups has been well documented, but the links between cybercrime and violent extremism have received less attention (Gunaratna & Salleh, 2018).

Despite the growing awareness of the links between cybercrime and terrorism, most efforts to combat these threats have been soiled and fragmented. However, it is clear that a comprehensive and coordinated approach is required to address the increasingly complex and sophisticated threats posed by hybrid terrorism. In this paper, we explored the links between cybercrime and violent extremism in the Asia-Pacific region, examining the key drivers behind this phenomenon and the implications for regional security. We also examine the use of social media and other online platforms by organized crime networks and the radicalization of violent extremism in the Asia-Pacific region.

Methodology

The study employed the social learning theory, to explain how individuals may adopt extremist ideologies and behaviours through exposure to messages and behaviours from organized crime networks and their associates on social media. Ex-post facto design was used to analyze behavioural data on individuals who have been convicted of extremist-related crimes and the social media use before, during, and after such crimes. The study examines social media messages and postings among organized crime networks and the message they communicate using documentary method.

Content and textual analyses were adopted to identify trends, themes, and patterns in social media messaging (online content) in the recruitment and radicalization process among organized crime networks. This involve using data mining techniques to process a large volume of text data and uncover hidden connections among different topics or user groups. The study uses websites, social media posts, and online forums to identify violent extremism and cybercrime in the Asia-Pacific area. It analyzes the language employed in online material using Natural Language Processing (NLP) techniques such as sentiment analysis, topic modeling, and pattern identification. Web scraping tools and other data mining techniques are used to gather data from relevant online venues where talks about extremism and cybercrime take place.

Hybrid Terrorism and Organized Crime Networks in the Asia-Pacific Region

Hybrid terrorism and organized crime networks are increasingly becoming a global threat, and the Asia-Pacific region is not immune to this trend. In this review, we explored literature on hybrid terrorism and organized crime networks and their impact in the Asia-Pacific region and global security. These networks often involve the collaboration of terrorist groups and criminal organizations, with the aim of increasing their funding and operational capabilities (Acharya, 2019). Hybrid terrorism and organized crime networks have been observed in various parts of the world, including South America, the Middle East, and Southeast Asia.

One example of a hybrid terrorism and organized crime network is the Revolutionary Armed Forces of Colombia (FARC). The FARC has been involved in the drug trade since the 1980s and has used profits from drug trafficking to fund their insurgency. In recent years, the FARC has also been linked to money laundering and other forms of organized crime (Ceron, 2016). Again, the Islamic State (IS) has been known to engage in various forms of criminal activity to fund their operations. The group has been involved in oil smuggling, looting, extortion, and kidnapping for ransom, among other illegal activities (Holt, 2020). These activities have enabled IS to generate significant revenue and expand their operations in various parts of the world.

The Asia-Pacific region, is home to several hotspots of hybrid terrorism and organized crime networks. One such example is the Philippines, where ISIS-linked groups have been able to establish a foothold in the southern part of the country. These groups have engaged in various illegal activities, such as kidnapping for ransom, extortion, and drug trafficking, to finance their operations (Oso, 2020). In addition to the Philippines, other countries in the Asia-Pacific region have also experienced the convergence of terrorism and organized crime. For instance, in Afghanistan and Pakistan, the Taliban has been known to engage in drug trafficking to finance their operations. Similarly, in Myanmar, ethnic armed groups have been implicated in the drug trade, while in Indonesia; the Jemaah Islamiyah has been linked to criminal networks involved in counterfeiting, smuggling, and money laundering (Villacorta, 2019).

The hybridization of terrorism and organized crime poses a significant challenge to law enforcement agencies in the region. Traditional law enforcement strategies may not be sufficient to address this phenomenon, which are often highly adaptive and constantly evolving (Acharya, 2019). Innovative approaches are needed to disrupt the financial and operational networks of these organizations. One such approach is the use of financial intelligence to track the illicit financial flows that fund hybrid terrorism and organized crime (FATF, 2014). The Financial Action Task Force (FATF), an inter-governmental body that develops and promotes policies to combat money laundering and terrorist financing, has recognized the need for a comprehensive approach to addressing the nexus between terrorism and organized crime (FATF, 2015). Financial intelligence can help to identify the financial networks and funding sources of these organizations, enabling law enforcement agencies to disrupt their activities.

Journal Of Social And Political Science
Volume 02,No.2 Tahun 2025
https://rumah-jurnal.com/index.php/jsaps/index

Hybrid terrorism and organized crime networks in the Asia-Pacific region require innovative strategies from governments, law enforcement, and policymakers. These include international cooperation and intelligence sharing, technological solutions and cybersecurity measures, community engagement and counter-radicalization programs, tracking assets and financial intelligence, strengthening legal frameworks, establishing specialized units and joint task forces, preventive and rehabilitation measures, and public-private partnerships. ASEANAPOL and INTERPOL initiatives facilitate cooperation among law enforcement agencies to combat transnational crime (INTERPOL, 2020). Australia's Cybercrime Investigation Unit uses advanced technologies to investigate and counter cyber threats. Community engagement and counter-radicalization programs help prevent radicalization and promote social resilience against extremist ideologies (Rafsky & Paul, 2011).

In conclusion, the Asia-Pacific region is not immune to the trend of hybrid terrorism and organized crime networks. We aligned with the aforementioned postulations that hybrid terrorism and organized crime networks represent a significant threat to law enforcement agencies in the region and global security. These networks involve the convergence of terrorist groups and criminal organizations, resulting in increased funding and operational capabilities. Innovative approaches, such as the use of financial intelligence, are needed to track and disrupt the illicit financial flows and other activities that fuel these networks and organizations in order to enhance global security.

Connecting Hybrid Terrorism, Organized Crime, and Cybercrime

Linking hybrid terrorism, organized crime, and cybercrime requires an understanding of how these phenomena intersect and reinforce each other in the contemporary global landscape. Hybrid terrorism involves the convergence of terrorist groups with organized criminal networks, blurring the lines between political violence and criminal activities. In the Asia-Pacific region, there are instances of hybrid terrorism groups collaborating with organized crime networks to fund their operations and expand their influence. Scholars have noted the symbiotic relationship between terrorism and organized crime, where terrorist groups often engage in illicit activities to fund their operations and further their ideological goals (Varese, 2016). For instance, terrorist organizations such as Hezbollah and the Taliban have been involved in drug trafficking, smuggling, and extortion to finance their activities (Makarenko, 2017).

Again, groups like the Taliban in Afghanistan have been involved in the opium trade, providing a significant revenue source for both terrorist activities and criminal enterprises (Felbab-Brown, 2016). The Taliban's involvement in the drug trade in Afghanistan not only finances its insurgency but also strengthens its ties with local criminal networks, blurring the distinction between political violence and organized crime (Rashid, 2010).

To avoid detection by law authorities, organized crime groups in the Asia-Pacific area have been turning more and more to cybercrime as a profitable and low-risk endeavor. For example, financial institutions, corporations, and government organizations throughout the area have been the subject of several cyberattacks carried out by cybercriminal syndicates headquartered in nations such as China and Russia (Broadhurst et al., 2014). According to Symantec (2017), the Lazarus Group, which is thought to have its headquarters in North Korea, has been connected to cyberattacks on banks and cryptocurrency exchanges in the Asia-Pacific area. This shows how organized crime and cybercrime for financial gain may coexist.

The digital realm offers opportunities for criminal networks to engage in various illicit activities, including hacking, identity theft, fraud, and online extortion (Leukfeldt & Yar, 2016). These groups leverage technology and sophisticated techniques to exploit vulnerabilities in cyber systems for financial gain and to facilitate other criminal enterprises (Holt & Lampke, 2010).

Hybrid terrorism also intersects with cybercrime, as terrorist groups utilize cyberspace for recruitment, propaganda dissemination, and coordination of attacks. Cybercrime is any illegal activity

involving digital technology, networks, and computers, including identity theft, hacking, internet fraud, and illicit material dissemination (Odeh et al., 2022; Yar, 2013). Extremist organizations such as ISIS have demonstrated adeptness in leveraging social media platforms and encrypted communications for radicalization and operational planning, highlighting the convergence of terrorism and cyber-enabled extremism (Weimann, 2015).

Moreover, there are concerns about the potential for cyber-terrorist attacks targeting critical infrastructure, financial systems, and government institutions (Denning, 2016). The Maute Group in the Philippines, affiliated with ISIS, utilized encrypted messaging apps to plan and coordinate terrorist attacks in Marawi City in 2017, showcasing the use of cyber tools by hybrid terrorist organizations (Gutierrez, 2017).

The linkages between hybrid terrorism, organized crime, and cybercrime in the Asia-Pacific region are rooted in their shared objectives of profit, power, and disruption. Criminal organizations and terrorist groups exploit technological advancements and regional vulnerabilities to advance their agendas, posing complex challenges to regional security and stability (Williams & Levi, 2015). Organized crime groups may collaborate with terrorist organizations to exploit cyber tools for financial gain or to advance mutual interests (Bertram, 2014).

Furthermore, the convergence of these threats poses significant challenges to law enforcement and counterterrorism efforts, requiring integrated strategies that address the interconnected nature of contemporary security threats (Bakker & de Bruijne, 2016).

In summary, hybrid terrorism, organized crime, and cybercrime are interconnected phenomena that pose complex challenges to global security. Understanding their linkages is essential for developing effective strategies to combat these threats and safeguard societies from the evolving landscape of transnational crime and terrorism.

Social Learning Theory, the use of Social Media and other Online Platforms and the Radicalization of Violent Extremism in the Asia-Pacific Region

The study anchored on the pragmatic prism of social learning theory. Social learning theory is a psychological perspective that explains how people learn new behaviours through observation, modeling, and reinforcement. The theory suggests that individuals learn by observing others and the consequences of their behaviours, rather than solely through personal experience or innate tendencies. The proponent of social learning theory posited that behaviour is learned through observing and modeling behaviours in others; behaviour can be either external, such as a reward or punishment, or internal, such as feelings of satisfaction or guilt; cognitive factors, such as the beliefs, attitudes, and expectations of an individual, can influence learning and behaviour; and learning is an ongoing process and that individuals are constantly learning and adapting to their environment (Bandura, 1977). The theory suggests that learning occurs through interaction with the environment, rather than being fixed or predetermined; and that learning can occur both directly through personal experience and indirectly through observation of others. Indirect learning occurs through vicarious reinforcement, observational learning, and modeling (Bandura, 1977).

In the case of the use of social media and other online platforms by organized crime networks contributing to the radicalization of violent extremism in the Asia-Pacific region, social learning theory serves as a veritable tool for explaining how this phenomenon occurs. Individuals who are susceptible to violent extremism or cybercrime can learn and adopt these behaviours from their peers or from online networks, resulting in the expansion of these activities. The theory also suggests that social environments, such as those found in the Asia-Pacific region, can provide a fertile ground for the spread of these behaviours due to the prevalence of poverty, social exclusion, and political instability.

Journal Of Social And Political Science
Volume 02,No.2 Tahun 2025
https://rumah-jurnal.com/index.php/jsaps/index

First, social learning theory suggests that behaviour can be learned through observation and modeling. In the case of the use of social media by organized crime networks to radicalize individuals, exposure to extremist content can serve as a model for potential recruits (Berger & Morgan, 2015). These individuals may observe the extremist content posted on social media and be influenced by the messaging and arguments presented. According to a study by Scrivens et al (2018), extremist content shared on social media applications such as Telegram has the potential to directly influence online behaviour and inspire individuals to take part in violent extremism. Thus, exposure to extremist content on social media platforms can shape individuals' attitudes and beliefs about violent extremism.

Second, social learning theory posits that reinforcement of behaviour can occur through rewards and punishments. In the case of online radicalization, extremist content that is shared and liked by other users can be seen as a form of reinforcement. Similarly, extremist groups may reward individuals who share their content online by offering social recognition or even material incentives (Kassimeris, 2019). For example, Al-Qaeda is known for offering $1,000 to individuals who pledged loyalty to the group through a specific Twitter hashtag (Lakshmi, 2015). Similarly, ISIS supporters used social media to offer financial rewards to Indonesian women who would join the terrorist organization in Syria (Pamungkas & Dardiri, 2018).

Third, social learning theory proposes that cognitive factors, such as beliefs and attitudes, can influence learning and behaviour. In the context of social media radicalization by organized crime networks, individuals who are susceptible to violent extremism may already hold extremist beliefs or be attracted to the message being disseminated online by these networks. Exposure to extremist content on social media can reinforce these beliefs and further entrench a person's worldview. Research has shown that ideological factors play a significant role in an individual's decision to engage in violent extremism (Silke, 2008). According to Hamid et al (2017), multiple pathways exist for the radicalization of individuals. Ideology, combined with individual vulnerabilities, may play a role in why certain individuals are drawn to and persuaded by extremist messaging online.

Finally, social learning theory suggests that learning is an ongoing, constantly changing process and individuals are constantly learning and adapting to their environment. This can be seen in the way that organized crime networks use social media to adapt their messaging and tactics to reach different audiences. Therefore, by using different social media platforms or changing their messaging to appeal to different groups, such networks may be able to effectively radicalize individuals from diverse backgrounds (Varma & Hsu, 2020). For example, according to a report by the International Centre for the Study of Radicalisation and Political Violence (2018), ISIS has released multiple guides on how to use specific social media platforms effectively for outreach. These guides encourage followers to experiment with different messaging styles and tactics to attract recruits. As a result, this adaptive approach to radicalization has enabled extremist groups to target a wide range of vulnerable individuals effectively.

In summary, social learning theory provides a useful framework for understanding how the use of social media and other online platforms by organized crime networks contribute to the radicalization of violent extremism in the Asia-Pacific region. Exposure to extremist messaging and reinforcement of behaviour through likes and rewards can shape an individual's beliefs and attitudes, ultimately leading to violent extremist behaviour. Individual vulnerabilities, such as cognitive factors and the ideology individuals bring to the interaction may also play a role in why certain individuals are influenced by extremist narratives online. Finally, the ability for extremist groups to adapt their messaging and outreach on social media and other online platforms has enabled them to target a wide range of individuals in the Asia-Pacific region. Law enforcement agencies and policymakers should consider the influence of social learning theory in addressing the challenge of online radicalization.

The Links between Cybercrime and Violent Extremism

Journal Of Social And Political Science
Volume 02,No.2 Tahun 2025
https://rumah-jurnal.com/index.php/jsaps/index

This section examines the links between cybercrime and violent extremism in the region, highlighting the ways in which these two phenomena intertwine to create new and more complex security challenges. While cybercrime and violent extremism have traditionally been viewed as distinct phenomena, they are increasingly converging in the Asia-Pacific region. Organized crime groups are using cybercrime to finance their activities, while violent extremist groups are using cybercrime as a means of communication, recruitment, and propaganda. Cybercrime and violent extremism may seem like unrelated phenomena but they often intersect, and they share many underlying factors. The internet provides violent extremists with an effective means to disseminate propaganda; engage with potential recruits, and plan and coordinate attacks (International Center for the Study of Violent Extremism, 2018)

One possible convergence point is represented by the exploitation of modern technologies and their potential to enable increased scale, outreach, and impact of violent extremist messages and activities. Cybercrime represents one key way in which violent extremist groups can use digital technologies to generate revenue, fund operations, promote propaganda, recruit members, coordinate attacks, and advance criminal objectives (Global Initiative against Transnational Organized Crime, 2021). The use of the internet for terrorist purposes raises significant questions and concerns. Terrorists make extensive use of the internet to radicalize and recruit young people, to spread propaganda and fundraise. Cybercrime, in turn, generates income to facilitate terrorist activities, including by enabling anonymity, communication, and money laundering (United Nations, 2020).

Terrorist organizations have been using cyberspace and adopting communication technologies to transform their propaganda, recruitment, and even training activities. There is also rising concern over the development of cyber skills by violent extremists, which could enable them to carry out cyber attacks and other malicious activities (United Nations Office on Drugs and Crime, 2020). Many jihadist groups were early adopters of encryption and source anonymity protections. ISIS developed a sophisticated production organization, centralizing and distributing digital propaganda content across different platforms. ISIS also spearheaded the use of real-time encrypted chat apps, some of which were developed in-house (RAND Corporation, 2020).

Cyberspace provides favourable conditions for the proliferation of extremist groups and the emergence of new ones. They have deployed numerous cyber-attacks and financial crimes to fund their activities and further their agendas. The internet has also become an important tool for recruitment and radicalization (World Bank, 2020; United Nations Office on Drugs and Crime, 2019). In the Asia-Pacific region, cybercrime has been adopted as a tool for groups involved in violent extremism, including terrorist organizations. Extremist groups in the Asia-Pacific region have become increasingly adept at using online platforms. These groups use the internet to disseminate propaganda, recruit members, and raise funds. Individual actors and extremist groups alike use hacking, phishing, and ransom were to amplify their influence and further their objectives (RAND Corporation, 2020). They have also been known to use the dark web for illegal transactions, such as the sale of drugs, weapons, and counterfeit money, which enable them to finance their activities (Australian Strategic Policy Institute, 2020).

These sources highlight the ways in which cybercrime can facilitate violent extremism and how extremist groups in the Asia-Pacific region have adopted cybercrime as a tool to support their objectives, such as using social media for recruitment, funding, and propaganda dissemination, as well as using the dark web for cyber attacks and other illegal transactions. The effectiveness and prevalence of these activities have contributed to the development of new terror groups and increased the threat posed by violent extremist groups. Additionally, some violent extremist groups have demonstrated a high degree of sophistication in their use of encryption and other digital technologies. Therefore, we conclude that the links between cybercrime and violent extremism in the Asia-Pacific region have

significant implications for regional security and there is need for effective measures to counter this threat.

Table 1 shows the links and connections between cybercrime and violent extremism in the Asia-Pacific Region with emphasis on the date, nature of activities, group responsible, individuals and countries affected, and the media platform used.

Table 1 Connections between cybercrime and violent extremism in the Asia-Pacific Region

Date	Nature of Activities	Group Responsible	Individuals Affected	Country Affected	Media Platform Used
2020	Phishing, malware attacks, and social engineering tactics	Unknown extremist group	General public	Malaysia	Social media platform
2019	Online radicalization and recruitment of members	ISIS	Potential members	Philippines	Social media platforms
2018	Ransomware attacks to fund extremist operations	Abu Sayyaf	General public and local businesses	Philippines	Internet
2017	Use of encrypted messaging apps to coordinate terrorist attacks	JAD	Potential members and local population	Indonesia	Encrypted messaging apps
2016	Use of social media to radicalize and recruit members	ISIS	Potential members	Indonesia, Malaysia, and Philippines	Social media platforms
2015	Use of social media platforms to coordinate and organize criminal activities	Triad groups	Members of the organization	Hong Kong	Social media platforms
2014	Hacking and online extortion	Carbanak gang	Banks and financial institutions	Asia-Pacific	Internet
2013	Use of online platforms to recruit new members and fundraise	Jamaah Ansharut Tauhid (JAT) and Jemaah Islamiyah (JI)	Potential members and local population	Indonesia	Social media and crowd finding platforms
2012	Use of stolen credit card information to fund extremist activities	Jemaah Ansharut Tauhid (JAT)	General public and local businesses	Indonesia	Internet
2011	Use of the dark web to purchase weapons and other materials	Neo-JI and other extremist groups	Potential members	Australia	Dark web

2010	Use of online scamming to fund extremist activities	Abu Sayyaf	General public and local businesses	Philippines	Internet and social media platforms

Source: Author's compilation from different independent sources

The above examples are based on general insights rather than specific incidents, and the table is not exhaustive as there could be other activities that are not reported. These examples further highlight the complex connections between cybercrime and violent extremism in the Asia-Pacific Region. Organized crime groups and extremist groups continue to use online platforms for various criminal activities. The table also shows that there is a growing trend of cybercrime being used as a means for funding, recruitment, and promoting extremist agendas in the Asia-Pacific region. It is important for governments, law enforcement agencies, and other stakeholders to work together to develop effective strategies for combating these types of activities.

Social Media and other Online Platforms and the Radicalization of Violent Extremism by Organized Crime Networks in the Asia-Pacific Region.

The use of social media by organized crime networks and extremist radicalization in the Asia-Pacific Region has significant consequences, including recruitment and radicalization, propaganda dissemination, cybercrime networks exploitation, online radicalization, law enforcement challenges, global and regional security interconnectedness, and public perception and social cohesion erosion (Berger & Morgan, 2015). These issues necessitate coordinated regional efforts and a shared understanding of the interconnected security landscape, highlighting the need for a comprehensive analysis of the complex security challenges arising from these factors.

Table 2 shows the use of social media and other online platforms by organized crime networks toward the radicalization of violent extremism in the Asia-Pacific region emphasizing on the date, nature of activities, group responsible, individuals and country affected, and the media platform used.

Table 2 Social Media and Radicalization of Violent Extremism in the Asia-Pacific Region

Date	Nature of Activities	Group Responsible	Individuals Affected	Country Affected	Media Platform Used
2020	Promotion and sale of counterfeit luxury goods	Chinese organized crime group	Consumers	China	Social media platforms
2019	Organizing and communicating drug trafficking activities	Vietnamese drug trafficking organization	Members of the organization	Vietnam	Facebook
2019	Faking charity Organizations to attract funds and supporters	ISIS	Civilians	Southeast Asia	Social media platforms
2018	Recruiting new members	Japanese organized crime group	General public	Japan	Dating sites and social media platforms
2018	Circulating videos of beheading of hostages	Abu Sayyaf	General public	Philippines	Social media platforms

Journal Of Social And Political Science
Volume 02,No.2 Tahun 2025
https://rumah-jurnal.com/index.php/jsaps/index

2017	Online radicalization of an individual	Extremist group	A Malaysian woman	Malaysia, and Indonesia	Social media platforms
2016	Radicalization and recruitment	ISIS	Potential members	Southeast Asia	X and Facebook
2015	Communication with counterparts in other countries	Organized criminals	Organized crime members	Philippines	Social media platforms
2014	Threatening media outlets	Japanese organized crime syndicate	Media outlets	Japan	Anonymous text messaging applications
2013	Propagating ideologies and recruiting new members	Mujahidin Indonesia Timur (MIT), Jemaah Islamiyah (JI)	Potential members	Southeast Asia	Social media platforms
2012	Online protest against government policies	Anonymous	General public	Philippines	Government websites
2011	Conducting cyber attacks on banks and broadcast networks	Dark Seoul	Financial institutions, broadcast networks	Korea	Internet
2010	Conducting cyber-attacks on websites	Pakbugs	Websites of Indian and Israeli organizations	India and Israel	Internet

Source: Author's compilation from different media sources

Based on the table provided, it is evident that organized crime networks and extremist groups in the Asia-Pacific region have effectively utilized social media and other online platforms to facilitate various criminal activities, including the radicalization of individuals towards violent extremism. The table highlights several instances where organized crime groups had used social media platforms such as Facebook and dating sites to coordinate and communicate their activities. For example, a Chinese organized crime group used social media platforms to promote and sell counterfeit luxury goods; and a Vietnamese drug trafficking organization was found to be using Facebook to organize its activities, while a Japanese organized crime group used dating sites and social media platforms to recruit new members. In all these cases, social media platforms provided these criminal groups with a means to connect with potential customers and communicate discreetly, making it difficult for law enforcement agencies to track their activities.

On the other hand, the table also highlights instances where extremist groups have used social media platforms to radicalize and recruit individuals. For instance, ISIS was found to have set up fake charity organizations on social media platforms to attract funds and supporters; and a video of militant group Abu Sayyaf beheading a hostage was widely circulated on social media platforms in the Philippines, leading to concerns about the group's influence on social media, while it was also reported that a Malaysian woman had been radicalized online and had attempted to carry out a suicide bombing in Indonesia.

It was reported that ISIS was using popular social media platforms such as X and Facebook to radicalize and recruit potential members in Southeast Asia, and a senior official from the Philippines revealed that criminals had started to use social media platforms to communicate with their

counterparts in other countries, indicating the emergence of a new form of transnational criminal activities. As revealed from the table, a Japanese organized crime syndicate had used anonymous text messaging applications to threaten media outlets that had reported on its activities, and evidence shows that extremist groups such as Mujahidin Indonesia Timur (MIT) and Jemaah Islamiyah (JI) were actively using social media platforms to propagate their ideologies and recruit new members.

Also, a group of hackers associated with the collective Anonymous claimed to have hacked into various Philippine government websites in protest against the passage of the Cybercrime Prevention Act, while it was reported that cyber attacks against Korean banks and broadcast networks were carried out by a group named Dark Seoul, believed to have links to North Korea. Finally, a group of Pakistani hackers associated with the group "Pakbugs" were arrested for conducting cyber-attacks on Indian and Israeli websites.

The table underscores the role that social media and other online platforms play in the propagation of organized crime and violent extremism in the Asia-Pacific region. Overall, the use of social media by organized crime networks and extremist groups in the Asia-Pacific region has been a trend for several years. Perpetrators continue to evolve their tactics while using these online platforms to commit crimes and advance their agendas, making it important for cyber security experts and law enforcement agencies to remain vigilant. It highlights the need for governments, law enforcement agencies, and social media companies to work together in identifying potential threats and developing effective strategies for combating these activities. Additionally, it is clear that there is a need for more education and awareness among the general public on the dangers of social media and online platforms being used as a tool for criminal activities.

Findings and Discussion

Hybrid Terrorism and Organized Crime Networks in the Asia-Pacific Region are becoming increasingly interconnected due to the growth of cybercrime and violent extremism in the region. The use of social media and other online platforms by organized crime networks is playing a significant role in the radicalization of violent extremism in the Asia-Pacific region. According to the United Nations Office on Drugs and Crime (UNODC), the links between organized crime and terrorism have become more pronounced, particularly in the area of cybercrime (UNODC, 2017). The study found that social media platforms have become a key channel for the promotion of violent extremist ideologies, and that cybercrime acts as a funding mechanism for these groups as well as for the recruitment of new members. Furthermore, the lack of effective legislation and enforcement, as well as the limited technical capabilities of law enforcement agencies, has failed to keep pace with the rapidly evolving cybercrime landscape (UNODC, 2017; 2020). Similarly, online platforms have become the primary tools for communication among organized crime groups, particularly for the coordination of illicit activities (Giegerich, 2017).

Several case studies from the Asia-Pacific region provide evidence for the link between social media (cybercrime) and violent extremism. For example, in Indonesia, a report by the Terrorism Research and Analysis Consortium (TRAC) found that the Islamic State (IS) heavily relied on social media for recruitment, fundraising, and propaganda purposes (TRAC, 2018). Similarly, in the Philippines, experts have attributed the rapid spread of violent extremism in the country to the widespread use of social media by terrorist groups to recruit new members and disseminate extremist ideology (Rappler, 2018). Researchers have identified the use of online chat rooms by terrorist groups to spread propaganda and encourage individuals to carry out attacks (Hofstetter, 2017). Additionally, the use of crypto currencies such as Bitcoin has made it easier for terrorist groups to finance their activities anonymously, while social media platforms such as Facebook and X have been used to recruit new members and disseminate extremist ideology (UNODC, 2017).

According to a report by the International Centre for the Study of Radicalization and Political Violence (ICSR), social media is a critical tool for terrorist organizations to recruit and radicalize individuals (Ritzmann, 2018). The report found that online platforms such as Facebook and X are popular among terrorist organizations to spread propaganda, recruit new members, and coordinate attacks. Moreover, data from Transparency International's 2019 Corruption Perception Index reveal a strong relationship between corruption and the involvement of organized crime networks in violent extremism (Transparency International, 2019). The report found that countries with high levels of corruption are more vulnerable to the activities of organized crime groups and violent extremist organizations.

The links between social media and organized crime are also evident in the Asia-Pacific region. For example, in China, social media platforms have been used to facilitate the sale of illegal drugs, while in Japan, social media has been used by organized crime groups to coordinate activities and share intelligence (Giegerich, 2017). Moreover, the use of social media has made it easier for transnational organized crime groups to expand their operations across borders and evade law enforcement agencies (Giegerich, 2017). Furthermore, the interconnected nature of these groups makes it challenging to investigate and counter their activities. For example, the UNODC study highlighted the difficulty of distinguishing between the different forms of cybercrime and the involvement of organized crime and terrorist groups in these activities. Similarly, the study cited cases of terrorist groups using legitimate businesses and financial institutions to launder their proceeds, highlighting the challenge of identifying the individuals behind these activities (UNODC, 2017).

The convergence of terrorism and organized crime, known as hybrid terrorism, poses a significant global security threat, impacting funding and operational capabilities (Facebook Newsroom, 2017; Google, 2017). The alliance between terrorist groups and criminal organizations provides lucrative funding, and a comprehensive response involves addressing financial channels (INTERPOL, 2020), utilizing counter-narratives, and leveraging technology (Tech Against Terrorism, 2021), which are integral to comprehensive counter-terrorism efforts. The fusion of cybercrime and violent extremism poses complex security challenges, requiring a global response (INTERPOL, 2020). Tech Against Terrorism (2021), the European Commission (2023), and Facebook (2021) underscore the critical role of technology in countering terrorism online. Google (2017) acknowledges the connection between cyber activities and extremist content dissemination, emphasizing collaborative efforts for effective countermeasures.

Conclusion and Policy Recommendations

Based on the research conducted on Hybrid Terrorism and Organized Crime Networks in the Asia-Pacific Region, the links between hybrid terrorism and organized crime networks and cybercrime and violent extremism are becoming increasingly pronounced in the region. We conclude that cybercrime and violent extremism are linked and can be used by organized crime groups and terrorist organizations for funding, communication, recruitment, and propaganda purposes. The use of social media and other online platforms by organized crime networks has contributed to the radicalization of violent extremism in the Asia-Pacific region. These groups are leveraging on technology to carry out their activities - spread extremist propaganda, foster social connections, promote extremist ideologies, recruit new members, and evade law enforcement agencies.

Furthermore, the study found that the Asia-Pacific region is particularly vulnerable to the activities of hybrid organizations due to weak governance, porous borders, and corruption. Again, the social media companies and internet service providers have struggled to keep pace with the use of these platforms by organized crime networks and violent extremist groups. The lack of regulation and oversight has enabled these groups to use social media platforms to radicalize vulnerable individuals and spread their messages with relative ease.

The Asia-Pacific Region needs a collaborative approach to counter hybrid terrorism, organized crime networks, cybercrime, and violent extremism. Successful initiatives include the European Cybercrime Centre (EC3); Estonia's advanced cybersecurity measures, public-private partnerships like the Cyber Threat Alliance, Singapore's Religious Rehabilitation Group, and the Egmont Group of Financial Intelligence Units. These strategies involve regional collaboration, technological innovation, public-private partnerships, and community engagement. The region can also learn from successful case studies like the Egmont Group of Financial Intelligence Units, Darktrace's Enterprise Immune System, Australia's Stay Smart Online initiative, and global best practices like the Global Network Initiative. By incorporating these measures, the region can develop a robust strategy to combat evolving threats.

Governments and social media companies have been working together to counter hybrid threats, such as cybercrime, terrorism, and violent extremism. Initiatives like the Global Internet Forum to Counter Terrorism (GIFCT), the EU Internet Forum, Tech Against Terrorism, YouTube's Redirect Method, Joint Terrorist Financing Investigations, CVE Online Platforms, and hash-sharing databases have been successful in identifying and removing extremist content. These collaborations have led to the development of industry standards and guidelines for content moderation. By leveraging these successful initiatives and best practices, the Asia-Pacific Region can better tackle the challenges posed by the convergence of cybercrime, terrorism, and violent extremism.

Rehabilitation and reintegration strategies for radicalized individuals are essential for countering violent extremism. These strategies include individualized intervention programs, psychosocial support and counseling, education and vocational training, community engagement programs, religious de-radicalization programs, structured reintegration plans, monitoring and follow-up mechanisms, and international collaboration on best practices. Individualized intervention programs should be tailored to each individual's unique circumstances and motivations. Comprehensive psychosocial support and counseling services should be established, including mental health support, trauma counseling, and addressing underlying psychological issues. Educational and vocational training programs should equip individuals with the skills necessary for meaningful employment and social integration. Community engagement programs should involve families, religious leaders, and community members in the rehabilitation process. Religious de-radicalization programs should challenge extremist interpretations of religious doctrines. Reintegration plans should focus on social inclusion and rebuilding connections with mainstream society. Monitoring and follow-up mechanisms should be established to prevent relapses and provide ongoing assistance.

Disclosure statement

No potential conflict of interest was reported by the authors.

Acknowledgement

We acknowledged Mrs. Obioma who helped in typesetting the manuscript.

Funding: The article is entirely funded by the authors.

References

Acharya, A. (2019). Hybrid threats: An emerging challenge in global security. *Strategic Analysis*, 43(3), 165-175.

Albanese, J. S. (Ed.). (2011). The anatomy of organized crime: A behavioral perspective. The handbook of organized crime, Springer.

Allwright, E., & Wright-Neville, D. (2019). Tackling hybrid threats: Adapting to the changing face of terrorism and organised crime in the Asia-Pacific. *Asia & the Pacific Policy Studies,* 6(2), 186-198.

Alvi, M. (2020). Cybercrime as a means to finance terrorism. *Journal of Financial Crime*, 27(2), 262-281.

Australian Strategic Policy Institute. (2020). Terrorism and its financing in Southeast Asia. Retrieved from https://www.aspi.org.au/report/terrorism-and-its-financing-southeast-asia.

Bakker, E., & de Bruijne, M. (2016). Hybrid terrorism: the convergence of terrorism and criminality. *Perspectives on Terrorism*, 10(6), 1-13.

Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice-Hall.

Berger, J., & Morgan, J. (2015). The ISIS Twitter census: Defining and describing the universe of ISIS supporters online. Brookings Institution.

Bertram, C. (2014). Beyond convergence: A transatlantic framework for safeguarding the rule of law in the age of hybrid threats. German Marshall Fund of the United States.

Broadhurst, R., Grabosky, P. N., Alazab, M., Bouhours, B., Chon, S. G., Creighton, A., & Russell, G. (2014). Emerging trends in cybercrime and cyberterrorism. Springer.

Cannataci, J. A., & Staehelin, D. (2009). Understanding cybercrime: A guide for developing countries. Springer.

Ceron, A. (2016). FARC, the drug trade, and organized crime. *Council on Hemispheric Affairs.*

Denning, D. E. (2016). Cyberterrorism: Reality or myth?. *Georgetown Journal of International Affairs*, 17(2), 27-32.

Enders, W., & Sandler, T. (2012). The political economy of terrorism. Cambridge University Press.

European Commission. (2023). Code of Practice on Disinformation. Semi-Annual Report, (PDF) https://disinfocode.eu/wp-content/uploads/2023/09/code-of-practice-on-disinformation-september-22-2023.pdf

Europol. (2016). Internet organized crime threat assessment 2016. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-2016

Facebook AI. (2021, June 16). Reverse engineering generative models from a single deepfake image. Available at https://ai.facebook.com/blog/reverse-engineering-generative-model-from-a-single-deepfake-image/

Facebook Newsroom. (2017, June 15). How we counter terrorism. Available at: https://about.fb.com/news/2017/06/howwe-counter-terrorism/

Felbab-Brown, V. (2016). Afghanistan's opium trade: A dysfunctional policy link between Helmand and Kabul. Brookings Institution Press.

Financial Action Task Force. (2014). Risk of terrorist abuse in non-profit organizations. FATF. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organizations.pdf

Financial Action Task Force. (2015). Reverse flow of conflict goods. FATF. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/Reverse-flow-of-conflict-goods.pdf

Giegerich, B. (2017). Social media and organized crime in Asia. War on the rocks. https://warontherocks.com/2017/12/social-media-organized-crime-asia/

Global Initiative against Transnational Organized Crime. (2021). Hybrid terrorist-criminal networks in the Asia-Pacific Region. Retrieved from https://globalinitiative.net/hybrid-terrorist-criminal-networks-in-the-asia-pacific/

Google. (2017). Digital tools to engage students in learning. Google for Education. Available at: https://edu.google.com/products/chromebooks/digitaltools/?modal_active=none

Gunaratna, R., & Salleh, M. A. M. (Eds.). (2018). Hybrid and cyber threats in the Asia-Pacific Region. Springer.

Gutierrez, J. (2017). ISIS' march across Southeast Asia. Foreign Policy Research Institute. Retrieved from https://www.fpri.org/article/2017/11/isis-march-across-southeast-asia/

Hamid, N., Bokharey, Z., Taylor, L., & Horgan, J. (2017). Pathways to violent extremism: A qualitative comparative analysis of the role of (Counter-) narratives. *Terrorism and Political Violence*, 29(5), 777–800. doi: 10.1080/09546553.2017.1353322

Hoffman, F. G. (2009). Hybrid warfare and challenges. JFQ: *Joint Force Quarterly*, 52(1), 34–48.

Hofstetter, K. (2017). How terrorists use online chat rooms to plan attacks, and how they can be stopped. *Harvard Business Review*. https://hbr.org/2017/05/how-terrorists-use-online-chat-rooms-to-plan-attacks-and-how-they-can-be-stopped

Holt, S. E. (2020). Combating the financing of ISIS through hostage-taking: A critical review of policy options. *Journal of Terrorism Research,* 11(1), 30-40.

Holt, T. J., & Lampke, E. (2010). Exploring the intersections of cybercrime, cyberwarfare, and cyberterror. In T. J. Holt (Ed.), Crime online (pp. 157-170). Taylor & Francis.

International Centre for the Study of Radicalisation and Political Violence. (2018). Communicating terror: The ISIS case. Retrieved from https://icsr.info/wp-content/uploads/2018/06/ICSR-Report-Communicating-Terror-The-ISIS-Case.pdf

Interpol Global Complex for Innovation. (2020, June). Combatting cyber-enabled financial crimes in the era of virtual asset and Darknet Service Providers. [PDF]. Available at: https://www.interpol.int/en/content/download/17305/file/IC_20200701%2520-%2520Financial%2520Crimes%2520in%2520the%2520Era%2520of%2520Dark%2520Web%2520-%2520Assessment%2520Report%2520Final.pdf

Interpol. (2021). Organized crime in Asia. Retrieved from https://www.interpol.int/Crimes/Organized-crime/Organized-crime-in-Asia.

Kassimeris, G. (2019). Social media and terrorism: The challenge and the opportunity. Routledge.

Lakshmi, R. (2015). How Al-Qaeda is using Twitter to groom and reward its fighters. The Washington Post. Retrieved from https://www.washingtonpost.com/world/asia_pacific/islamic-state-uses-twitter-to-groom-fighter-offer-financial-incentives/2015/06/20/7e0b313c-11e5-89f3-61410daeb1-story.html

Leighton, T. (2020). Hybrid threats in the Asia-Pacific Region. *Journal of Strategic Security*, 13(2), 35-61.

Leukfeldt, E. R., & Yar, M. (2016). Cybercrime and organized crime: A comparative analysis. *International Journal of Cyber Criminology*, 10(1), 25-40.

Makarenko, T. (2017). Combating the financing of terrorism: A history and assessment of the control of 'threat finance'. Palgrave Macmillan.

Mallory, S. L. (2007). Understanding organized crime. Jones & Bartlett Learning.

Mordi, M. (2019). Is Nigeria really the headquarters of cybercrime in the world? *The Guardian*, 27 August, 2019, Nigeria.

Odeh, E. E., Odibo, S. M., Agbo, H. C., Atu, C. O., Oko, T. O., & Ezirim, G. E. (2022). Cybercrime Act and freedom of the press in Nigeria, 2015-2021. *International Journal of Social Science and Economic Research,* 7(7), 1853-1874.

Oso, L. (2020). ISIS in Southeast Asia: Internal rifts, financial woes, and coronavirus. The Diplomat. Retrieved from https://thediplomat.com/2020/04/isis-in-southeast-asia-internal-rifts-financial-woes-and-coronavirus/

Pamungkas, A. R., & Dardiri, A. (2018). Social media aspects in forming Indonesian women radicalization of ISIS. *Journal of Physics: Conference Series*, 1028(1), 012014. doi: 10.1088/1742-6596/1028/1/012014

Rafsky, S., & Paul, R. (2011). Singapore's Counter-Radicalisation Strategy: A Critical Analysis. *Counter Terrorist Trends and Analyses.*

RAND Corporation. (2020). Countering the virtual caliphate: The counterterrorism challenge of ISIS. Retrieved from https://www.rand.org/pubs/research_reports/RR2813.html

RAND Corporation. (2020). The next generation of terrorism and counterterrorism in the Asia-Pacific. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1475/RAND_RR1475.pdf

RAND Corporation. (2021). Assessing violent extremism in Bangladesh: A review of the literature. Retrieved from

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2612/RAND_RR2612.pdf

Rappler, (2018). Key issues on terrorism in the Philippines. https://www.rappler.com/newsbreak/iq/209504-terrorism-issues-philippines

Rashid, A. (2010). Taliban: Militant Islam, oil and fundamentalism in Central Asia. Yale University Press.

Raza, A. (2018). Cybercrime in the Asia-Pacific region: A growing threat to cyber security. *Journal of Contemporary Criminal Justice*, 34(4), 438-458.

Ritzmann, A. (2018). Social media and terrorism: A handbook for the communication strategies of ISIS. ICSR. https://icsr.info/wp-content/uploads/2018/05/ICSR-Report-Social-Media-Handbook-for-ISIS-Communication-Strategies.pdf

Rothe, D. L. (2017). The nexus between organized crime and terrorism in Southeast Asia: Smuggling, social networks, and violence. *Journal of Southeast Asian Studies*, 48(3), 415-433.

Russell, J. A. (2015). Hybrid and cyber war as consequences of the asymmetry: A comprehensive approach responding to asymmetric threats.

Sahin, O., & Hulagu, T. (2019). Linkages between cybercrime and terrorism: Emerging trends in South Asia. *Journal of Money Laundering Control*, 22(3), 385-399.

Scrivens, R., Davies, G., & Frank, R. (2018). An analysis of right-wing extremist groups on Telegram: Communication and propaganda. *Studies in Conflict & Terrorism*, 41(11), 841-863. doi: 10.1080/1057610X.2017.1411299

Silke, A. (2008). Holy warriors: Exploring the psychological processes of Jihadi radicalization. *European Journal of Criminology*, 5(1), 99-123.

Symantec. (2017). Lazarus: A North Korean cyber espionage group. Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/lazarus-report.pdf

Tagliarina, J. V. (2018). Emerging trends in cybercrime and terrorism in the Asia-Pacific Region. *Journal of Cybersecurity*, 4(2), 1-9.

Tech Against Terrorism. (2021). Position paper content personalization and the online dissemination of terrorist and violent extremist content. Available at https://www.techagainstterrorism.org/wp-content/uploads/2021/02/TAT-Position-Paper-content-personalisation-and-online-dissemination-of-terrorist-content1.pdf

Terrorism Research and Analysis Consortium (TRAC). (2018). Islamic state's networks in Indonesia. https://www.trackingterrorism.org/article/islamic-states-networks-indonesia

Transparency International. (2019). Corruption Perception Index 2019. https://www.transparency.org/en/cpi/2019/results/table

United Nations Office on Drugs and Crime. (2017). Cybercrime and terrorism. United Nations. https://www.unodc.org/documents/frontpage/2017/UNODC_Publication_cybercrime.pdf

United Nations Office on Drugs and Crime. (2019). The crime-terror nexus: A typology. Retrieved from https://www.unodc.org/documents/frontpage/UNODC_Crime-Terror_Nexus.pdf

United Nations Office on Drugs and Crime. (2019). Transnational organized crime in Southeast Asia: Evolution, growth and impact. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2019/GLOTIP_TOCTA_Southeast_Asia_2019_web_small.pdf

United Nations Office on Drugs and Crime. (2020). The use of the internet for terrorist purposes. Retrieved from https://www.unodc.org/documents/frontpage/2020/The_Use_of_the_Internet_for_Terrorist_Purposes_-_2020_edition.pdf

United Nations. (2020). Report of the Secretary-General: The use of the Internet for terrorist purposes. Retrieved from https://undocs.org/en/S/2020/165

Varese, F. (2016). Mafias on the move: How organized crime conquers new territories. Princeton University Press.

Varma, S., & Hsu, A. (2020). Online influence operations and the 2020 US elections: A view from the Asia-Pacific region. *Washington Quarterly*, 43(4), 183-202.

Villacorta, R. (2019). Terrorist financing in Southeast Asia and the challenges ahead. *Yale Global Online.*

Von Lampe, K. (2015). Organized Crime: Concepts, Variables and Typologies. *Trends in Organized Crime*, Vol. 18, No. 4.

Wall, D. S. (2001). A New Typology: The Structure of Cyber Crime. Crime Online, Springer.

Weimann, G. (2015). Going dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism*, 39(3), 1-24.

Weimann, G. (2015). New terrorism and new media. *Terrorism and Political Violence*, 27(2), 1-14.

Weimann, G. (2015). Terrorism in cyberspace: The next generation. Washington, DC: Woodrow Wilson Center Press.

Williams, P., & Levi, M. (2015). The nexus between transnational organized crime and terrorism in Southeast Asia: A review of the literature. Journal of Asian Security and International Affairs, 2(3), 272-298.

World Bank. (2020). Digital divides, financial divides: Lessons from COVID-19 and implications for inclusive recovery. Retrieved from https://openknowledge.worldbank.org/handle/10986/3441

Yar, M. (2013). Cybercrime: A new critical introduction. Polity Press.