Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

The role of digital distrust, negative emotion and government policy on cyber violence during the digital era in Indonesia

Mohammad Fadil Imran[a*] and Hendra Gunawan[a]

[a]*Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia*

C H R O N I C L E

Article history:
Received: January 6, 2024
Received in revised format: February 20, 2024
Accepted: May 2, 2024
Available online: May 2, 2024

Keywords:
Digital Distrust
Negative emotions
Government policy
Cyber Violence
PLS-SEM
Indonesia

A B S T R A C T

In the digital era the research study discusses the role of government policy, negative emotions and digital trust in cyber violence, therefore this research adds to the literature and provides references regarding the important role of government policy on cyber violence is very limited. This research aims to investigate the relationship between digital distrust and cyber violence, and the relationship between government policy and cyber violence. The research method used in this research is associative research. Associative research is research that aims to determine the relationship between the hubs of two or more variables. In this way, we can build a theory that functions to predict and control a phenomenon. The population in this study were all students who had studied using e-learning or digital platforms. In this study, the number of respondents was 543 high school students throughout Indonesia. The sampling technique used in this research is nonprobability sampling. In this research, the data collection method used was the questionnaire method. The instrument used to measure this research variable is a 5-point Likert scale. Data processing in this research uses SmartPLS software. The stages of data analysis in this research are the outer model test which includes convergent validity, discriminant validity and composite reliability as well as inner model analysis, namely hypothesis testing. The results of this research are that digital distrust has a positive and significant relationship to cyber violence, negative emotions have a positive and significant relationship with cyber violence, and government policy has a positive and significant relationship with cyber violence. This research adds to the literature and provides references regarding the important role of government policy, digital distrust, and negative emotions in cyber violence. Indonesia, the government needs to implement and evaluate new regulations related to cybercrimes. The government must establish new regulations to combat cybercrime.

1. Introduction

In this digital era and industrial revolution, cybercrime is increasing due to technological developments. The government's job is to bring digital technology and provide facilities to the people, but little attention is given to preventing global cybercrime (Alotaibi et al., 2022). Crime agencies have reported an increase in violence in the digital world, with some people using digital platforms to discriminate against people on social media. Violence in the cyber world has a psychological impact on victims. Along with increasingly sophisticated technological developments, the level of risk and threat of misuse of information and communication technology is also increasingly higher and more complex. Cybercrime occurs more easily and has become a priority issue for all countries in the world today. The increase in digital economic and financial activities not only has a positive impact on the Financial Services Industry in Indonesia but also brings cyber security threats that have the potential to pose major risks. Based on data from the National Cyber and Crypto Agency (BSSN), the largest cyber-attacks during 2023 occurred in the financial sector (23%), manufacturing industry (17.7%) and energy sector (10.2%). Kominfo data

* Corresponding author.
E-mail address mfadilimran@stik-ptik.ac.id (M. F. Imran)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2024.5.001

states that throughout 2023 there will be 888,711,736 cyber threats recorded in Indonesia. This figure is equivalent to 42 cyber threats per second. Cybercrime is a crime committed via the internet network or computers via an internet network that can infiltrate users (Sharma et al., 2021). Types of cybercrime that often occur include hacking, phishing, cyberbullying, cyber-stalking, and many more. This crime can cause major losses for individuals and companies who have been affected by this crime. In the industrial era 4.0, where almost all activities are carried out digitally, this creates a large opportunity for this crime to occur as the biggest threat to current technological developments. Not only is it financially detrimental, but cyber-crime can also damage a company's reputation and threaten user privacy so that digital crime can destroy a group or individual itself (Turan et al., 2011). The potential risk of cybercrime is still a threat lurking in the country's financial services sector in 2024 (Backe et al., 2018). Reflecting on the previous year, it is deemed necessary to pay attention to the company's internal resource capacity to anticipate or minimize risks related to the threat of cybercrime. Indonesian Financial Group (IFG) Pro-gress, in Economic Bulletin Issue 43 entitled Risk Portrait in the Financial Services Sector and Real Sector in 2023, which was released at the end of 2023, found that the aspect of data and information security or cybercrime was the highest risk in the financial services sector, both in terms of its potential and impact on business. Several factors make it easier for cybercrime to occur, including Unlimited internet access (Wu, 2022). Nowadays, the internet can be easily used by everyone. This allows people to access everything without any restrictions, making it easier for criminals to carry out their actions. Cybercrime crimes will increase significantly in 2023 when compared to the same period in 2022.

Cybercrime is a crime related to computers or network devices, usually, this crime is committed online. This cybercrime can target anyone. If you become one of the victims, it will certainly cause a lot of harm. It even affects your mental condition and even financial losses (Baek et al., 2019). The objectives of this action are very diverse. Starting from threats, blackmail, humiliating someone and taking advantage of others. Along with the rapid progress of technology and the internet, the threat of cybercrime is increasingly emerging. To protect ourselves from various cyber-attacks, of course, we must know how to minimize them. Cybercrime, also known as cybercrime, is a form of crime that occurs in cyberspace via computers, mobile devices and internet networks. The perpetrators of these cybercrimes are generally 'smart people' who understand how computer algorithms and programming are run. Through certain algorithms, perpetrators can easily analyze, look for loopholes, and then ultimately break into our devices. When the perpetrator has control of the device, the perpetrator can freely steal our data and use it for the perpetrator's gain. Cybercrime is a crime related to computers or network devices, usually, this crime is committed online. This cybercrime can target anyone. If you become one of the victims, it will certainly cause a lot of harm. Cybersecurity is an effort made to maintain confidentiality, integrity, and availability of information in cyberspace (Berson et al., 2002). Cyberspace refers to a complex environment which is the result of interactions between people, software and services on the internet, which is supported by information and communication technology (ICT) devices and network connections spread throughout the world. Meanwhile, According to Blaya et al. (2018), cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Cybersecurity is usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or disrupting business process operations (Alotaibi et al., 2022).

The development of information and communication technology has led to new media in the form of the Internet which has caused world relations to become borderless and caused significant social, economic, and cultural changes. Human life today is very dependent on technology (Baek et al., 2019). On the one hand, technology can bring many positive impacts, such as E-mail, E-commerce, Cyberbanking, Online Business, Internet Banking, and so on. However, on the other hand, it also hurts the emergence of cybercrime. The dynamics of advances in information and communication technology today, apart from having a positive impact, also have a negative impact due to the inappropriateness of its use which results in the emergence of a crime known as cybercrime. Understanding Cybercrime is a new phenomenon in crime as a direct impact of the development of information technology by using the internet as a medium for committing crimes (Brantly et al., 2017). Technological advances have implications for the development of crime. A crime that was previously considered a crime if there was physical contact between the perpetrator and the victim when committing a crime has transformed into a crime in cyberspace or cybercrime which can be committed without direct physical contact between the perpetrator and the victim using the internet and other electronic devices. The impact of the internet provides opportunities for criminals to commit more hidden crimes that can penetrate time and space with a wide reach, even globally (Berson et al., 2002; Sari & Camadan, 2016).

2. Literature Review

2.1 Cyber Violence

According to Cheung et al. (2009), digitalization has changed the lives of traditional people to modern ones, people who use digital technology are involved in violence in cyberspace. The information provided on platforms is not safe because many people can access the information. Many children and women have become victims of violence due to the misuse of digital technology. Behavior that falls into the category of sexual harassment on social media includes the following: Cyber Stalking is the act of stalking using the internet, email or online messages. Cyber Harassment is harassing behavior that creates an intimidating, hostile, or offensive environment. Implementing effective cybersecurity is now a challenge because there are so many more devices than users, and attacks are becoming more innovative (Blaya et al., 2018). Even though the supporting infrastructure for cyber security has been strengthened nowadays, this does not rule out the possibility of an exponential increase in cyber security threats. Seeing the urgency of cybersecurity, serious efforts are needed from organizations to build

a reliable data and information security infrastructure, and competent personnel, and develop standard operational procedures for managing data and information by referring to cybersecurity standards. Bullying is any form of oppression or violence carried out intentionally by one person or group of people who are stronger towards another person, to hurt and is carried out continuously. The difference. Cyberbullying is carried out by utilizing digital technology. According to Cho and DioGuardi (2020) and Cho et al. (2021), Cyberbullying can occur on social media, online message exchange platforms, and via mobile phones. Like bullying, cyberbullying is repeated behavior aimed at expressing unfounded anger, frightening, and humiliating someone. It takes various forms, such as spreading fake news, uploading photos or videos that embarrass someone, sending messages containing hate speech, and impersonating someone to commit a crime through a fake account (Berson et al., 2002).

2.2 Digital Distrust

Distrust of digital due to violence in cyberspace, people use social media to share information that is not used or not needed on social media. According to Cripps and Stermac (2018), Children and girls who are victims of digital distrust have psychological problems, problems that are negative for children's development. Meanwhile, the negative impact of social media is that it distances people who are close and vice versa, face-to-face interactions tend to decrease, making people addicted to the internet, causing conflict, privacy problems, and being vulnerable to the bad influence of other people. Social media use also has negative impacts that need to be considered: Cyberbullying: Teenagers are vulnerable to online harassment and intimidation (Mkhize et al., 2020). Cyberbullying can have a detrimental impact on their emotional well-being, causing stress, anxiety and even depression. Judging from the legal aspect, those who commit crimes because of social media will be subject to criminal sanctions. Crimes result from social media via Facebook, for example, someone can commit a crime because they are provoked by the status on social media, causing disputes that lead to fights, assaults, and even murder. In this case, if the perpetrator is a minor or teenager, they can be charged with a crime (Owen, 2016). Based on the literature, the following hypothesis is formulated:

Hypothesis 1: *Digital Distrust has a positive and significant relationship with Cyber Violence.*

2.3 Negative Emotions

Negative emotions occur due to distrust of digital platforms. Some victims of violence on digital platforms have attempted suicide, the use of vulgar language and negative comments are increasing on social media platforms, and most people have used fake profiles to carry out cybercrime activities. According to Crespi and Hellsten (2022), Psychological impacts: easy depression, anger, feelings of restlessness, anxiety, self-harm and suicidal thoughts. Social impact: withdrawal, loss of self-confidence, more aggression towards friends and family. Although bullying is more common face-to-face, bullying can also occur in cyberspace, including on social media. This condition is known as cyberbullying. This negative impact of social media is usually triggered by differences of opinion in the comment's column, which then leads to long debates and acts of cyberbullying (Lallie et al., 2021). When this happens, victims of cyberbullying can experience mental health problems, such as stress and depression. even triggering suicidal thoughts. As for forms of crime in cyberspace or what is often called Cyber Crime, there are several types of crime in cyberspace such as hacking, cracking, spamming and so on. Especially among teenagers who still cannot regulate their use (Owen, 2016). Many cases of bullying among teenagers on social media occur because there is no control, thereby changing the behavior of teenagers who are victims in the real world to become unlike themselves. Just like on the social media Facebook, perpetrators can easily express opinions or words that lead someone to harm other Facebook users (Shaheen et al., 2023). If the victim does not accept what the perpetrator conveys, there will be retaliation which can be carried out in the real world. Even if the victim does not have the power to respond to the bullying that befell him, it could have worse consequences, including committing suicide. This is one of the initial triggers for a form of crime or crimes committed by teenagers because of bad use of social media. Based on the literature, the following hypothesis is formulated:

Hypothesis 2: *Negative emotions have a positive and significant relationship with Cyber Violence.*

2.4 Government policy

According to Durán and Rodríguez-Domínguez (2023), another way to overcome cybercrime is to improve the skills of human resources in Indonesia. Indonesia needs to work together with other parties or countries to improve its ability to handle cybercrime. Moreover, currently technological developments have begun to shift to blockchain technology, the government must be able to understand and know how to control the potential threat of cybercrime through this technology. Apart from improving skills, the government also needs to build a secure digital infrastructure system (Sharma et al., 2021). With a solid cyber security system, cybercrime can be prevented. Development of this system must begin with technology updates to accommodate new cyber threats. Cyber Law will be the legal basis for the law enforcement process against crimes using electronic and computer means, including money laundering crimes and terrorism crimes. In other words, Cyber Law is needed to tackle cybercrime. ITE Law As a legal approach to cyber security, Indonesia has an Information and Electronic Transaction Law to prevent cybercrime, but this law still needs to be re-evaluated because many articles are less relevant. Cyber Law is needed, in efforts to prevent criminal acts, as well as handling criminal acts (Turan et al., 2011). Cyber Law will be the legal basis in the law enforcement process against crimes using electronic and computer means, including money

laundering crimes and terrorism crimes. Cyber Security and Cyber Defense have at least one close connection, namely that both are applied to maintain and maintain confidentiality, integrity and availability of electronic information or Electronic Systems. Cyber Security can be a form of Cyber Defense. On the other hand, Cyber Defense can be either active defense or passive defense. The passive defense in question can be covered within the scope of Cyber Security. Cyber Security and Cyber Defense can be carried out by individuals, collectives, or countries (Wu, 2022). Each scope can be different. Cyber Security and Cyber Defense organized by the state are intended to maintain the confidentiality, integrity, and availability of important information for the state and national security, as well as safeguard Electronic Systems that are strategic or critical for the continuity of public services or the continuity of the state (Peterson & Densley, 2017). Based on the literature, the following hypothesis is formulated:

Hypothesis 3: *Government policy has a positive and significant relationship with Cyber Violence.*

3. Method

The research method used in this research is associative research. Associative research is research that aims to determine the relationship between two or more variables. In this way, we can build a theory that functions to predict and control a phenomenon. The population in this study were all students who had studied using e-learning or digital platforms. In this study, the number of respondents was 543 high school students throughout Indonesia. The sampling technique used in this research is nonprobability sampling. In this research, the data collection method used was the questionnaire method. The instrument used to measure this research variable is a 5-point Likert scale. Data processing in this research uses SmartPLS software. The stages of data analysis in this research are the outer model test which includes convergent validity, discriminant validity and composite reliability as well as inner model analysis, namely hypothesis testing.

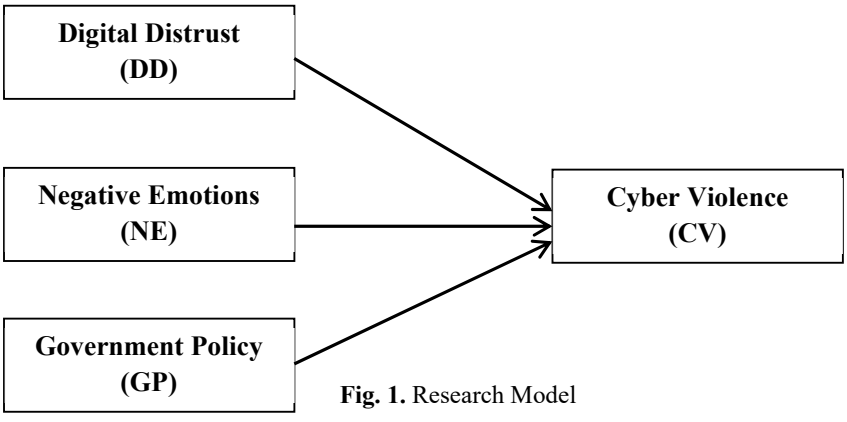

Fig. 1. Research Model

4. Results and Discussion

4.1 Validity and Reliability Test

To obtain the reliability and validity values of the research, loading factor, convergent validity, Cronbach alpha and composite reliability and average variance extracted (AVE) tests were carried out. Based on Table 1, the Cronbach alpha value for all variables was greater than 0.70, and the loading factor value for all indicators was greater than 0.70. greater than 0.70, the composite reliability value for all variables is greater than 0.70 and the average variance extracted value for all variables is greater than 0.60, so it is concluded that this research meets the validity and reliability requirements.

Table 1
Loading Factors, Cronbach Alpha, CR and AVE

		Factor Loadings	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted
Digital Distrust	DD1	0.903	0.801	0.824	0.802	0.783
	DD2	0.907				
	DD3	0.913				
Negative Emotions	NE1	0.939	0.823	0.890	0.805	0.718
	NE2	0.926				
	NE3	0.925				
Government Policy	GP1	0.920	0.818	0.823	0.823	0.765
	GP2	0.906				
	GP3	0.862				
Cyber Violence	CV1	0.925	0.789	0.835	0.891	0.734
	CV2	0.930				
	CV3	0.943				

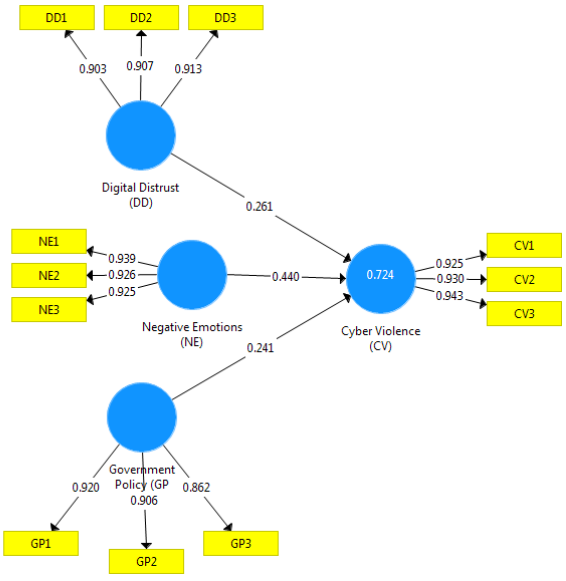

Fig. 2. PLS Algorithm Measurement Model

4.2 Discriminant validity

The discriminant validity test is used to check the discriminant between measurement scales in research. The Heterotrait-Monotrait (HTMT) discriminant validity limit value cannot be greater than 0.90.

Table 3
Discriminant Validity

	Digital Distrust	Negative Emotions	Government Policy	Cyber Violence
Digital Distrust				
Negative Emotions	0.864			
Government Policy	0.812	0.765		
Cyber Violence	0.789	0.632	0.712	

4.3 Hypothesis testing

Based on the analysis of the data that has been processed, the results can be used to answer the hypothesis in this research. Hypothesis testing in this research was carried out by looking at the t-statistic values and probability values. The research hypothesis can be declared accepted if the t statistic is > 1.96 and the probability value is < 0.05. The following are the output results from SmartPLS which are shown in Table 3 and Fig. 2.

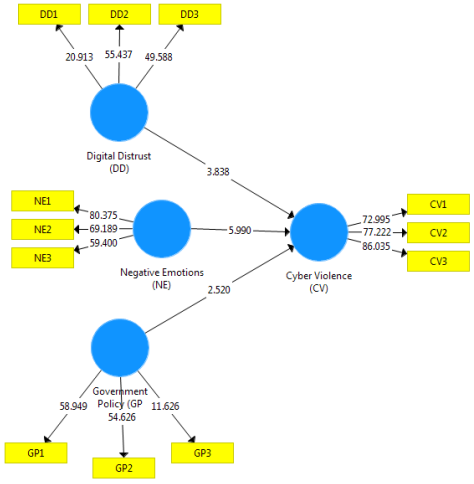

Fig. 3. Hypothesis Testing Bootstrapping

Table 4
Hypothesis Testing

Correlation	Original Sample	t Statistics	P-Values	Result
Digital Distrust → Cyber Violence	0.261	3.838	0.000	Significant
Negative Emotions → Cyber Violence	0.440	5.990	0.000	Significant
Government Policy → Cyber Violence	0.241	2.520	0.000	Significant

4.3.1 The relationship between digital Distrust and cyber violence

Based on the PLS-SEM results, the p-value is 0.000, so it can be concluded that digital distrust has a positive and significant relationship with cyber violence. These results are in line with Yaqub et al. (2022) that digital distrust has a positive and significant relationship to cyber violence and is supported by Hassan et al. (2020) that digital distrust has a positive and significant relationship to cyber violence. Distrust of digital is the cause of cybercrime and violence in cyberspace. Distrust of digital due to violence in cyberspace, people use social media to share information that is not used or not needed on social media. Children and girls who are victims of digital distrust have psychological problems, problems that are negative for children's development (Fernet et al., 2023). Meanwhile, the negative impact of social media is that it distances people who are already close and vice versa, face-to-face interactions tend to decrease, making people addicted to the internet, causing conflict, privacy problems, and being vulnerable to the bad influence of other people (Kričkić et al.,2017). Social media use also has negative impacts that need to be considered: Cyberbullying: Teenagers are vulnerable to online harassment and intimidation. Cyberbullying can have a detrimental impact on their emotional well-being, causing stress, anxiety and even depression.

4.3.2 The relationship between negative emotions and cyber violence

Based on the PLS-SEM results, the p-value is 0.000, so it is concluded that negative emotions have a positive and significant relationship with cyber violence. These results are in line with Kričkić et al. (2017) that negative emotions have a positive and significant relationship to cyber violence is supported by Lian et al. (2022) that negative emotions have a positive and significant relationship to cyber violence. People with negative emotions are more dangerous because they lack emotional intelligence. In cyberspace, negative emotions include regret, anxiety, and fear. Cyberattacks can cause the spread of negative positions and trigger cyber violence. Negative emotions occur due to distrust of digital platforms. Some victims of violence on digital platforms have attempted suicide, the use of vulgar language and negative comments are increasing on social media platforms, and most people have used fake profiles to carry out cybercrime activities (Li, 2023). Psychological impacts: easy depression, anger, feelings of restlessness, anxiety, self-harm and suicidal thoughts. Social impact: withdrawal, loss of self-confidence, more aggression towards friends and family (Lee et al., 2022).

4.3.3 The relationship between government policy and cyber violence

Based on the PLS-SEM results, the p-value is 0.000, so it is concluded that government policy has a positive and significant relationship with cyber violence. These results are in line with Stevens et al. (2021) that government policy has a positive and significant relationship to cyber violence and is supported by Lee et al. (2022) that government policy has a positive and significant relationship to cyber violence. Law enforcement in dealing with cybercrime in Indonesia has not been implemented optimally. Factors that will influence law enforcement against cybercrimes include legal factors, law enforcement factors, means and facilities in law enforcement and community factors. Of these four factors, the factor that has the most influence on the weakness of existing law enforcement in overcoming cybercrimes in the anatomy of transnational crime is the legal factor (legal substance) which contains many weaknesses and law enforcement factors. Second, the policy of criminalizing acts in cyberspace must continue to harmonize with the rise of crime in an increasingly sophisticated cyber world. This is due to criminal acts of information technology that do not recognize territorial boundaries and operate virtually (Fernet et al., 2023). Therefore, the government must always try to anticipate new activities regulated by applicable law. The first step in improving cybersecurity is increasing awareness among the public. The government has a responsibility to create an environment that supports cyber security. By creating relevant regulations and policies, the government can direct the private sector and society towards better security practices. Collaboration between the government and the private sector is the key to success in facing growing cyber threats. According to Shaheen et al. (2023), The government also has a role in providing resources and training to build cybersecurity capacity among the public and IT professionals.

According to Mkhize et al. (2020), cybercrime is a serious threat to the digital security and privacy of individuals, businesses and governments throughout the world. The COVID-19 pandemic has accelerated technology change and adoption across the world. In recent years, technology has become an Internal part of everyday life and social activities, and the pandemic has also strengthened this trend. Therefore, individuals and organizations need to pay attention to cyber security and take the necessary measures to protect themselves from cybercrime threats (Lee et al., 2022). Some actions that can be taken include using the latest security software, updating the system regularly, securing internet connections, using strong and unique passwords, and backing up data regularly. Additionally, it is important to remain alert to suspicious messages or phone calls and always verify the authenticity of an email or message before clicking on a link or submitting personal information. In a

pandemic situation, ensuring cyber security will help protect individuals and organizations from cybercrime threats, as well as ensure the smooth running of activities in cyberspace. According to Owen et al. (2016) To overcome this problem, there needs to be cooperation between the government, companies, and society in protecting themselves from crimes in cyberspace. Several ways can be done to avoid this IT crime, including strengthening the security system on internet networks and computers as a group or individually. Increase public awareness regarding the importance of protecting themselves from crimes in cyberspace, thereby reducing the occurrence of these crimes. Implement strict regulations for companies operating in the technology sector to prevent crimes in cyberspace (Lian et al., 2022). Developing more sophisticated and safe security technology to protect users from crime in cyberspace. To overcome the problem of cybercrime in the industrial era 4.0, there needs to be awareness and cooperation from all parties. In this way, technological developments can run safely and avoid the threat of cybercrime. Preventing online violence cannot be separated from the role of the government and policymakers. It is necessary to conduct a comprehensive study regarding policies on social media. Starting from the age restriction feature, limiting sensitive content, as well as providing complaints against violence that occurs on social media. To overcome cybercrime, the government still must strengthen its regulations and digital infrastructure. Apart from that, facing the threat of crime cannot be done by one institution alone. Education about the dangers of cyber threats also needs to continue to be echoed through any media so that people are more familiar with digital (Lee et al., 2022).

Indonesia needs a national cyber security strategy in the current era of society 5.0. If security is freedom from threats or dangers, one of the most important drivers in managing cyber security is how threats are understood in cyberspace and then solutions are sought. Without proper cyber security efforts, the likelihood of threats will increase. According to Šincek et al. (2017), the biggest challenges currently are strengthening cyber security institutions, the absence of a legal basis for cyber security and the lack of professional staff and cooperation within the country and internationally. So, the government needs to strengthen cyber security and prepare the people needed in an increasingly digital world. The Cyber Security Law must also be passed as quickly as possible to start Indonesia's national security efforts against the increase in cyberattacks in the current era of society 5.0. There are several problems related to the strategy to strengthen cyber security, including 1) Weak understanding of state administrators regarding security related to the cyber world, which requires restrictions on the use of services whose servers are located abroad and requires the use of secured systems, 2) Legality of handling attacks in the cyber world. , 3) The pattern of cybercrime incidents is very fast so it is difficult to handle, 4) National cyber security institutional governance is still limited, 5) Low awareness or awareness of the threat of international cyberattacks which can paralyze a country's vital infrastructure and 6) The industry is still weak in the country to produce and develop hardware or hardware related to information technology which is a gap that can strengthen or weaken security in the cyber world

5. Implications

This research implies that there has been no significant research discussing the role of government policy, negative emotions and digital trust in cyber violence, therefore this research adds to the literature and provides references regarding the important role of government policy on cyber violence. For the government and stakeholders to reduce crime cases in Indonesia, the Government needs to implement and evaluate new regulations related to cybercrime. The government must establish new regulations to combat cybercrime. The government must collaborate with non-government organizations to prevent cybercrime. The cyber security strategy that Indonesia must implement to realize national security in the era of Society 5.0, is by 1) capacity building for all stakeholders, 2) Establishing a Special Law on Cyber Crime to create legal certainty for cyber security in Indonesia, 3) Increasing resources humans by educating and recruiting professional staff who have integrity and good ethics to support strengthening cyber security. 4) Collaboration with domestic stakeholders through multi-stakeholders and international cooperation in developing and strengthening the capacity of cyber security capabilities both for infrastructure, infrastructure and in developing resource capabilities in the field of cyber security. In this digital era, children's safety in cyberspace is a major concern for parents. In an increasingly connected and online world, the risk of violence in cyberspace is also increasing. Children are often the targets of various acts of violence such as cyberbullying, grooming, or misuse of personal information by irresponsible people. For this reason, maintaining children's digital security is a very important task for all parents. In this era of rapid information, children have easier access to interact with the online world. However, as parents, we must realize that the internet is not always safe and enjoyable. It is important to prevent violence in cyberspace so that our children can explore the digital world safely and comfortably. Ultimately, maintaining children's digital security is a shared responsibility between parents and children. By taking appropriate preventive steps and guiding children to use the internet wisely, we can help them explore cyberspace safely and comfortably. Let's commit to maintaining our children's digital security so that they can grow and interact healthily in an increasingly wide digital world.

6. Conclusion

The results of this research are that digital distrust has a positive and significant relationship to cyber violence, negative emotions have a positive and significant relationship to cyber violence, and government policy has a positive and significant relationship to cyber violence. Human resources are one of the most important elements in ensuring the implementation of cyber security, by established policies. Special knowledge and skills must be possessed and maintained by developments in security needs. Human resources are realized in the form of recruitment, coaching and separation programs that refer to applicable regulations. In the digital era like now, cyberbullying or intimidation via social media is increasingly rampant. Almost everyone has likely experienced or witnessed this incident. Therefore, the role of emotional regulation becomes very important

in dealing with this problem. Emotional regulation or the ability to control and manage emotions is key to overcoming cyber-bullying. Individuals who can regulate their emotions well tend to be able to respond to intimidation more wisely, thereby reducing the potential for conflict that endangers themselves or others. If emotional regulation is not carried out properly, aggression or anger arising from cyberbullying has the potential to trigger dangerous actions, such as retaliation or even violence. Therefore, learning how to regulate emotions is very important in dealing with bullying in the digital world. This research is limited to students in Indonesia; therefore, respondents need to be expanded to other countries, further research should use different methods such as qualitative and mixed methods.

References

Alotaibi, N. B., & Mukred, M. (2022). Factors affecting the cyber violence behaviour among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA. *Technology in Society, 68*, 101863.

Backe, E. L., Lilleston, P., & McCleary-Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyber violence. *Violence and gender, 5*(3), 135-146.

Baek, H., Roberts, A. M., Seepersad, R., & Swartz, K. (2019). Examining negative emotions as mediators between exposures to family violence and bullying: A gendered perspective. *Journal of school violence, 18*(3), 440-454.

Berson, I. R., Berson, M. J., & Ferron, J. M. (2002). Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States. *Journal of School Violence, 1*(2), 51-71.

Blaya, C., Kaur, K., & Sandhu, D. (2018). Cyberviolence and cyberbullying in Europe and India. Bullying, cyberbullying and student well-being in schools: Comparing European, Australian and Indian perspectives, 83-106.

Brantly, A. F. (2017). The violence of hacking: state violence and cyberspace. *The Cyber Defense Review, 2*(1), 73-92.

Cheung, A. S. (2009). A study of cyber-violence and internet service providers' liability: lessons from China. *Pacific Rim Law & Policy Journal, 18*, 323.

Cho, Y., & DioGuardi, S. (2020). Strain, negative emotion, and cyber violence among South Korean juveniles: a mediation analysis. *Children and Youth Services Review, 108*, 104601.

Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review, 121*, 105840.

Cripps, J., & Stermac, L. (2018). Cyber-sexual violence and negative emotional states among women in a Canadian university. *International journal of cyber criminology, 12*(1), 171-186.

Crespi, I., & Hellsten, L. A. M. (2022). Cyberviolence and the digital experience: reflections on a problematic issue for youth. *International Review of Sociology, 32*(3), 391-399.

Durán, M., & Rodríguez-Domínguez, C. (2023). Sending of unwanted dick pics as a modality of sexual cyber-violence: an exploratory study of its emotional impact and reactions in women. *Journal of interpersonal violence, 38*(5-6), 5236-5261.

Fernet, M., Hébert, M., Brodeur, G., Guyon, R., & Lapierre, A. (2023). Youth's Experiences of Cyber Violence in Intimate Relationships: A Matter of Love and Trust. *Journal of child sexual abuse, 32*(3), 296-317.

Hassan, F. M., Khalifa, F. N., El Desouky, E. D., Salem, M. R., & Ali, M. M. (2020). Cyber violence pattern and related factors: online survey of females in Egypt. *Egyptian journal of forensic sciences, 10*, 1-7.

Kričkić, D., Šincek, D., & Babić Čike, A. (2017). Sexting, cyber-violence and sexually risk behaviour among college students. Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju, 25(2), 15-28.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security, 105*, 102248.

Lian, Y., Zhou, Y., Lian, X., & Dong, X. (2022). Cyber violence caused by the disclosure of route information during the COVID-19 pandemic. *Humanities and social sciences communications, 9*(1), 1-18.

Li, X. (2023). The Causes of the Cyber Violence Problem Taking Qzone as an Example. *Journal of Education, Humanities and Social Sciences, 11*, 22-27.

Lee, Y., Kim, J., & Song, H. (2022). Do negative emotions matter? Paths from victimization to cyber and traditional bullying from a General Strain Theory perspective. *Crime & Delinquency, 68*(13-14), 2503-2528.

Mkhize, S., Nunlall, R., & Gopal, N. (2020). An examination of social media as a platform for cyber-violence against the LGBT+ population. *Agenda, 34*(1), 23-33.

Owen, T. (2016). Cyber-Violence: Towards a Predictive Model, Drawing upon Genetics, Psychology and Neuroscience. *International Journal of Criminology and Sociological Theory, 9*(1), 1-11.

Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here?. *Aggression and violent behavior, 34*, 193-200.

Sari, S. V., & Camadan, F. (2016). The new face of violence tendency: Cyber bullying perpetrators and their victims. *Computers in human behavior, 59*, 317-326.

Šincek, D., Duvnjak, I., & Milić, M. (2017). Psychological outcomes of cyber-violence on victims, perpetrators and perpetrators/victims. *Hrvatska revija za rehabilitacijska istraživanja, 53*(2), 98-110.

Shaheen, H., Rashid, S., & Aftab, N. (2023). Dealing with feelings: moderating role of cognitive emotion regulation strategies on the relationship between cyber-bullying victimization and psychological distress among students. *Current Psychology, 42*(34), 29745-29753.

Sharma, M. K., Anand, N., Thakur, P. C., NS, B. A., & John, N. (2021). Cyber violence: case report evidence of an emerging public health concern. *Asian Journal of Psychiatry, 57*(102017), 10-1016.

Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking, 24*(6), 367-376.

Turan, N., Polat, O., Karapirli, M., Uysal, C., & Turan, S. G. (2011). The new violence type of the era: Cyber bullying among university students: Violence among university students. *Neurology, psychiatry and brain research, 17*(1), 21-26.

Wu, X. (2022). Analysis of the relationship between college students' cyber violence news and cyber violence behavior in social media. *International Journal of Frontiers in Sociology, 4*(11), 40-44.

Yaqub, R. M. S., Siddique, H. M. A., Gillani, S. F., & Murad, M. (2022). Moderating role of Government Policy into the Relationship between Digital Distrust, Negative Emotions, Information Overload and Cyber Violence: Evidence from Pakistan. *Pakistan Journal of Humanities and Social Sciences, 10*(3), 1121-1131.