# SYNERGY, SYSTEM IT, RISK MANAGEMENT AND THE INFLUENCE ON CYBER TERRORISM AND HOAX NEWS ACTION

[1]TIGOR SITORUS, [2]HENDY TANNADY

[1]Indonesian Police Science College, Indonesia
[2]Universitas Pembangunan Jaya, Indonesia

[1]sitorus_tigor@yahoo.com, correspondence author
[2]hendytannady@gmail.com

## ABSTRACT

This study aims to investigate the factors hoax and cyber terrorism also variables that influence the acts of cyber terrorism in the jurisdiction of the Republic of Indonesia National Police. The research approach uses mixed methods with triangulation analysis and multiple regression analysis while surveys, interviews and focus group discussions were conducted on 1078 personnel and the stakeholders in Jakarta, West Java, East Java, Bali and North Sumatra. The Normality Test shows the data is normally distributed and the hypothesis test using multiple linear regression analysis shows; 1) The Influence of Synergy on the Acts of Cyber Terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is negative and significantly with the perception of respondents who show that the implementation of synergy is good, 2). The Influence of IT Systems on the Acts of Cyber Terrorism and Hoax is negative and significantly, with the perception of respondents showing that the implementation of synergy is good. 3). Influence of Risk Management on the Acts of Cyber terrorism and Hoax is negative and significantly, with the perception of respondents who show that the implementation of risk management is good. 4). Simultaneously the influence of Synergi, IT System, Risk Management toward Cyber Terrorism and Hoax Actions with propaganda, agitation, doctrine, jihadist indicators is negative and significantly, meaning that if Synergi, IT System, Police Risk Management are good, then cyber terrorism acts in the form of Jihadists decreased significantly. 5). The synergy of prevention, Police Information Technology System, Risk Management, Simultaneously have a negative and significantly effect on cyber terrorism and hoax, so As a major finding that hoax typology is very varied and public perceptions about synergy, IT systems and risk management implemented by the Indonesian Police are good enough and significantly influence toward Cyber Terrorism and the spread of hoax news.

Keywords: *Synergi, IT System, Risk Management, Terrorism, Hoax*

## 1. INTRODUCTION

### 1.1. Background

Globalization and Millennialization actually have an impact on the opening of a country like Indonesia from various international influences such as the use of virtual or virtual-based information technology. The use of cyberspace in addition to positive objectives, apparently also for the purpose of terrorizing a government and society as well as the spread of hate speech and hoax news. As stated by Howard and Parks [27] that social media is media that consists of three parts, namely: Information infrastructure and tools used to produce and distribute media content, Media content can be in the form of personal messages, news, ideas, and Cultural products in the form of digital, then those who produce and consume media contents in digital form are individuals, organizations, and industries.

As one of the most densely populated countries in the world, it cannot be separated from this problem, there has been a surge in cyber crime cases from 2015 to 2019. According to Fitria [31], during 2019, the Indonesian Police handled 2,800 cyber cases. As many as 35 percent of them are cases of hoaxes and hate speech, the majority of which are related to elections. "Approximately 1,005 cases were cases related to hate speech, hoaxes, fake news, threats. While Dista Amalia Arifah [17] also Astuti and Sri Ayu [6] state that stated as the development of the internet then led

to the development of new communication media that shifted from conventional media to social media and communication that contained crime content. Even acts of terror are very easy to utilize internet-based communication media. As a result of acts of terror that are often launched through the internet, a new term of the crime has arisen, namely cyber terrorism by Ahmad and Yunos [5]. Meanwhile Seib & Janbek [29] in Eska Nia Sarinastiti and Nabilla Kusuma Vardhani [18] stated that a group of terrorists used cyberspace (various Internet applications) in carrying out their terrorist acts. The internet makes it possible to spread information quickly, with little risk, and is cheap in a variety of constituencies, from potential recruitment to the potential to find prospective partners in terrorist organizations, Seib & Janbek, [29].
As with the statement of the National Police Chief Tito Karnavian [32] stated during a hearing with the House of Representatives Commission III, "there were 31 one terrorism cases from 2015 to June 2017. Of these cases, there were 336 suspects arrested. Most of the suspects were arrested during the prevention process. So if we look at 336 suspects mostly in the process of prevention than arrest but it is exposed if it has exploded. From these two years, the pattern of terrorism has begun to change and now it is moving alone and radicalized through the internet. Through this internet also, the perpetrators can train their followers for attacking opponents, bomb and others without face to face communication.

There has been a change in the ways and patterns and acts of terrorism, thus encouraging the Indonesian National Police to change and process it, which is about encouraging interventions to become virtual by increasing the work of police officers based on information technology as well as taking steps to improve the Cyber Terrorist communication system and spread false news. This step is followed by counter measures in cyberspace, and also provides for the strengthening of safety, human resources and infrastructure, as well as building collaborative relationships with related relationships.
Cybercrime is a development of computer crime. Indonesia as one of the countries with the intensity of spreading, terrorism and hoaxes in the form of propaganda, agitation, doctrine, jihadists has increased significantly and colored news on social media especially ahead of the Presidential and Regional Election 17 April 2019 through the platform; Facebook, Twitter, Instagram, Whatsapp, Email, Line, Telegram and SMS, this study in line with J.A. Scholte [24].
In reality, the working patterns of conventional terrorism and cyber terrorism are very different. Although it does not eliminate human life and physical destruction, cyber terrorism has a significant impact on public services and for the future of civilization and world peace. Cyber terrorism cases have occurred in Indonesia in April 2004, namely the official website of the KPU (General Election Commission) which experienced hacking with destructive techniques, but soon the culprit, one can be secured by the police, although there are still many other cyber criminals who have not be identified.
In dealing with cyber terrorists, in fact the government really needs qualified technology and capable human resources. This is in line with Ineu Rahmawati [22] which states that the era of globalization encourages some countries to no longer use traditional and conventional war methods, but requires more modern methods. As a result, state power is no longer seen in the strength of weaponry, but also in terms of culture, economy, politics and technology, also synergy by Chin, Anantharaman et al. [10] and risk management by COSO [11].

### 1.2. Formulating of Problem

With the above explained background, so this paper states the main problem, namely; "How to prevent acts / terrorism and hoax news using cyber space.
In answering the above concern, this paper will look at the following specific issues:

1) What is the forms and quantity of cyber terrorism and hoaxes in the jurisdiction of Indonesia (?)
2) Does the synergy of prevention partially between institutions has a negative and significant effect on cyber terrorism and hoaxes?
3) Does the Police Information Technology System partially has a negative and significant effect on cyber terrorism and hoaxes ?
4) Does Risk Management partially has a negative and significant effect on cyber terrorism and Indonesian hoaxes ?
5) Do the synergy of prevention, Police Information Technology System, Risk Management Simultaneously have a negative and significant effect on cyber terrorism and Indonesian hoaxes ?

## 2. LITERATURE REVIEW

### 2.1. Cyber Terrorism

In essence, the term cyber-terrorism was first introduced by Denning[16], He defines cyber-terrorism as a combination of things related to cyberspace with terrorist acts. Study that mention above in line with Eska Nia Sarinastiti and Nabilla Kusuma Vardhani [18] also Collin, B. L. Collin [12] that examined the use of the Internet and Terrorism and the Strengthening of Global Cyber-Terrorism Actions through New Media.

Furthermore, Bambang A.S and Idealisa Fitriana [9] also Galamas, Francisco, [19], said that Cyberterrorism was an activity and / or method used by terrorist networks or groups. It is undeniable that cyberspace and technological advances easily become a place for them to carry out their actions. In realizing national resilience, a comprehensive response is needed to deal with the threat of misuse of information and communication technology (cyber threat / asymmetric threat for the benefit of terrorist acts). Meanwhile, according to the National Police Agency of Japan [25], cyber terrorism is an electronic attack through computer networks against critical infrastructure that has great potential to disrupt the social and economic activities of the nation. The US Department of Justice states that cyber terrorism is all illegal activities related to knowledge computer technology and according to the OECD (Organitation for Economic Co-operation and Development) cyber terrorism, namely illegal unethical or illegal behavior related to the automatic processing of data transmission. Understanding of cyber terrorism actually consists of two aspects, namely cyber space and terrorism, while the perpetrators are called cyber terrorists. Hackers and crackers can also be called cyber terrorists, because often the activities they do in cyberspace (the Internet) can be terrorized and cause huge losses to victims who are targeted, much like terrorist acts. Both of them exploit cyberspace (internet) for their respective interests such as the dissemination of information and hate speech or hoaxes. Perhaps the slight difference between cyber terrorists and hackers is only on motivation and purpose, where the motivation of cyber terrorists is for the political interests of certain groups with the aim of showing their existence on the world political stage. While the motivation of hackers is to show their existence or intelligence contest to show their superiotas in the world. While pursuing Dorothy Denning [16], namely: Cyberterrorsim is the convergence of cyberspace and terrorism. This definition refers to acts against the law by attacking and threatening to carry out attacks on computers, networks and information stored therein for the purpose of intimidating or coercing the government or society for political or social purposes.

From the various definitions above, cyberterorism and hoax distribution are the use of information technology in the form of internet networks as a means to commit crime. In this case the Internet as an organizational tool that functions as a tool for planning, giving command, communicating between group members. In addition, the information technology base becomes an important part of terrorism, namely as a propaganda media for terrorist activities.

### 2.2. Hoax

Hoax is an attempt to deceive or outsmart readers or listeners to believe it even though the owner of the news knows that the news is a lie with the intention of forming and driving public opinion and forming public perception and it is called hoaks which means false news as stated by Harley, D. [21] and Dedi Rianto Rahadi [15]. Hoax is a negative excess of freedom of speech and opinion on the internet. Especially social media and blogs. Hoax aims to create public opinion, lead opinions, form perceptions, also for fun that tests the intelligence and accuracy of internet users and social media. The emergence and development of hoaxes is made by a person or group with a variety of objectives, ranging from just playing games, to goals economics (fraud) and politics propaganda / formation of public opinion, Abdul Karim and Firdaus Wajdi [2] or agitation (demagoguery). Hoaxes usually arise when an issue sticks to the surface, but many things have not been revealed or become a question mark. The other reason is to become a viral Social media users also understand that Hoax information can divide the nation as stated by Judhita [14]. People are ore likely to believe Hoax if the information is in accordance with opinions or attitude owned, stated by Respati [28].

### 2.3. Synergy

Covey [13] defines synergy as a combination or a combination of elements or parts that can produce better or synergize, meaning combining our strengths with the power of others to work, not to compete or bring down. Synergy is not merely talking about differences, but instead it is strong with various similarities, synergy is also not only in the realm of communication but a lot of play in the realm of action. so synergy is more than just working together. Synergy is to create solutions or ideas that are better and more innovative than a collaboration. Therefore it is stated as a creative cooperation. Furthermore, Chin, Anantharaman et al. [10] suggested that employee performance is a collaboration of opportunities, efforts and abilities of employees can be determined from the work of the employee. While Ivancevich et. al [23], show that employees are willing high to work together to help the progress of an organization that has work performance higher.

### 2.5. Information Technology System

Information systems are computer applications to support the operation of an organization: the operation, installation, and maintenance of computers, software, and data. A computer-based information system is a collection of computer hardware and software designed to convert data into useful information. Understanding information systems according to O'Brien [26], information systems can be a regular combination of people, hardware, software, communication networks, and data resources that collect, change, and, spread information in an organization. While information technology is a technology used to support end users in obtaining the required information. Understanding of information technology according to O'Brien [26], hardware, software, telecommunications, database management, and other information processing technologies used in computer-based information systems. Meanwhile, according to Turban et.al. [30], that certain components of computer-based information systems are; software, hardware and brainware.

### 2.4. Risk management

Risk management is a structured approach / methodology in managing uncertainty related to threats; a range of human activities including: Risk assessment, development of strategies to manage it and mitigate risks using empowerment / resource management.

According to the Committee of Sponsoring Organizations of the Treadway Commission or COSO [11], risk management is a process carried out by the board of directors, management and other personnel, applied in strategy setting and throughout the company, designed to identify potential events that can affect the entity, and managing risk, to provide adequate confidence, regarding the achievement of the entity's objectives.

Ineu Rahmawati [22] states that risk faced in overcoming the threat of cyber crime is not inferior to conventional warfare. Thing this causes the identified risks to be able to produce a national defense strategy in facing the threat of cyber crime.

Based on previous theory and research, the following research model images are presented below:

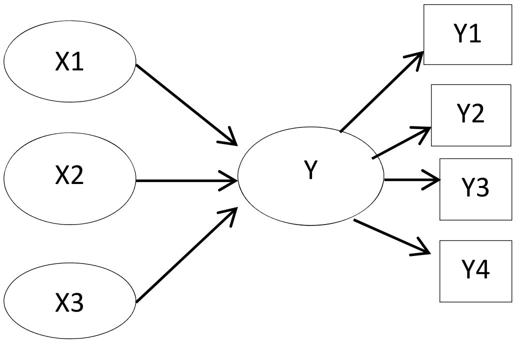

*Figure 1: Research Model*

Notes:
X1 = Synergy
X2 = Information and Technology System (SYS_IT)
X3 = Management of Risk (MRISK)
Y = Cyber Terrorism Action and Hoax news
Y1 = Propaganda
Y2 = Doctrine
Y3 = Agitation
Y4 = Jihadist

Where as; X1,X2,X3 are the independence variables, and “Y” is the variables dependence that influenced by the independence variables. While Y1, Y2, Y3, Y4 are the dimension of “Y” as variables dependence.

## 3. METHOD

### 3.1 Research Approach

This research activity is carried out with a mix method by Allison Shorten and Joanna Smith [1], where the data collection uses a qualitative and quantitative approach. A quantitative approach such as; documentation of various secondary data related to the research and distribution of questionnaires, which are also supported by qualitative data collection through in-depth interviews with competent parties, as well as conducting focus group discussions by Agusta Ivanovich [7].

The study was conducted in the jurisdiction of the Jakarta Police, the Bali Police, the East Java Police, the West Java Police and the North Sumatra Police with a sample of 1087 people from the approximately 50.000 population.

### 3.2 Research Instruments

The instrument used was a questionnaire. The questionnaire contained a number of questions from the indicators of all the research variables. Validity test is done to find out whether the measuring instrument used is able to measure what you want to measure with the minimum limit of validity of a measuring instrument with a magnitude of r 3 0.3. Therefore, if the correlation between items and factors is <0.3, then the items in the instrument are declared invalid.

The reliability test is intended to determine the minimum level of trust that can be given to the seriousness of the respondents' answers, which will be measured using construct reliability if the amount is > 0.70. shows the data is reliable that stated by Ghozali, Imam [20].

### 3.3. Research variable

The Variables In This Research Consist Of Independent Variables Namely System IT by O'Brien [26], Risk Management by COSO [11] and Synergy, Chin, Anantharaman et al. [10]. While Dependent Variables Are Cyber Terrorism And Hoax Indicated By Propaganda, Agitation, Doctrine And Jihadists, Abdul Karim and Firdaus Wajdi [2], Propaganda and Da'wah in Digital Era (A Case of Hoax Cyber-Bullying Against "Ulama").

### 3.4. Data collection technique

In essence, this research is an explanatory study by testing the model of the influence of independent variables on the dependent variable, so that empirical evidence is expected to be obtained by collecting data through questionnaires, collecting documents related to variables, and supported by in-depth interview data and conducting focus group discussion activities (FGD).

### 3.5 Analysis Method

Before analyzing the effect of independent variables on the dependent variable, it is best to first ensure the normality of the data with the normality test. In this study using the Kolmogorov-Smirnov parametric test technique. Furthermore, the authors used a multilevel linear regression analysis technique using SPSS 19 by Ghozali, Imam [20].

## 4. RESULTS AND DISCUSSION

### 4.1 Tests of Normality Data

Testing for normality through graph analysis Probability plot can be seen from the point of spread around the diagonal line. Normality test results can be seen in the following tabel.

*Table 1 Normality Test*

| | | Cyber Terrorist and Hoax | Synergi | Syste m IT | Risk Management |
|---|---|---|---|---|---|
| N | | 1078 | 1078 | 1078 | 1078 |
| Norma Parameters[a,l] | Mear | 78,47 | 78,45 | 36,28 | 37,82 |
| | Std Deviatior | 19,012 | 5,191 | 5,582 | 5,683 |
| Mos Extreme Differences | Absolute | ,152 | ,263 | ,076 | ,089 |
| | Positive | ,152 | ,169 | ,076 | ,086 |
| | Negative | -,127 | -,263 | -,070 | -,082 |
| Kolmogorov-Smirnov Z | | 1,044 | 1,003 | ,521 | ,534 |
| Asymp. Sig. (2-tailed) | | ,225 | ,223 | ,949 | ,959 |

*Source : Output SPSS 19*

The normality test results in the table above show that The Cyber Terrorist and Hoax is normally distributed with Kolmogorov-Smirnov value Z = 1.044 p = 0.225 (p> 0.05), Synergi data also normally distributed with Kolmogorov-Smirnov value Z = 1.003 p = 0.223 (p >0.05) while System IT is normally distributed with Kolmogorov-Smirnov value Z =0.521 p = 0.949 (p> 0.05) and Risk Management also normally distributed with Kolmogorov-Smirnov value Z =0.534 p = 0.959 (p> 0.05). The Normal data gives the meaning that the respondents' answers are spread evenly and not grouped on certain answers, so that the linearity of the influence of independent variables on the dependent variable will be obtained.

### 4.2. Variable description

From the questionnaire data collection, obtained a description of the answers based on respondents' perceptions as in the table below.

*Table 2 Respondents' perceptions of variables*

| NO | Variable | Agree-Strongly Agree (already good) | Disagree (already not good) |
|---|---|---|---|
| 1 | Synergy | 76% - 82% | 18 - 24% |
| 2 | IT System | 58% - 64% | 36 - 42% |
| 3 | Risk Management | 60% - 67% | 37 - 40% |
| 4 | Cyber Terrorism & Hoax Actions | 80%- 85 % * | 15 - 20%* |

*Source: Output SPSS19*

* Existence of Cyber Terrorism & Hoax Action

Based on Table 2, it can be seen that the Synergy Variable between The Indonesian National Polic functions and with the stakeholder shows that the average is good, where respondents agree and strongly agree around 76% -82%, except for the readiness of adequate IT facilities and facilities, only 58-64%, while A qualified Risk Management is still considered moderate with a score of 60% - 67%. While the respondents' perception score on the Terrorism and Hoax Acts in the form of propaganda, agitation, doctrination, jihadists is really real and makes the cyber climate not conducive by those who try to disturb the stability of national and state security through cyberspace / cyber high around 80% -85%.

### 4.3. Description of Terrorism and Hoax

Based on the results of triangulation of interview data, study of documents and observations collected by researchers, and carried out focus group discussion on primary data by Andriana Deni [3], obtained data and information that;

1) The intensity of the spread, terrorism and hoax has increased significantly and colored the news on social media especially ahead of the Presidential and Regional Election on April 17, 2019 through the platform; Facebook, Twitter, Instagram, Whatsapp, Email, Line, Telegram and SMS.
2) While the Hoax Typology that colors the flow of social media in Indonesia consists of; a). Proper Hoax is a hoax with the same title and content and is not based on strong and valid facts and data; b). Hoax titles are hoaxes with incorrect titles and are different from the news content; c). Disguise hoax is news hoax by presenting news / events that are old and not relevant at the moment.
3) Social media platforms that are often used by news disseminators, terrorism and hoaxes in each jurisdiction of Resort Police are very varied, among which the most prominent are; Facebook, Twitter and Instagram. Gates of incoming and outgoing content and news, terrorism and hoaxes are relatively numerous and make it difficult for cyber troops and cyber patrols to anticipate and detect quickly and optimally, so that they encounter obstacles to counteract at the first opportunity that is faster.
4) Resort Police still prioritizes the factual presentation approach in counter news, terrorism and hoaxes through; Narrative contra and upload of the success of the Government and the National Police, while Netizens who have ideological ideals must be approached with an emotional approach through figures considered being in line with netizens.
5) Resort Police's Human Resource with a background in IT education both at the Non Commissioned Officer and First Commissioned Officer levels, especially those serving at the Cyber Troops task force are still classified as "Rare" so that knowledge of the IT system is still self-taught that is difficult to adapt to changes in the IT system so quickly, while the appointment of personnel at the cyber troops task force is still "convenience =", and less selective based on passion and talent and educational background relevant to the field of duty, consequently less creative personnel develop their duties and work in counteracting news, terrorism and hoaxes. This carries the risk of weakness in preventing and exposing cyber terrorism and hoax news dissemination.
6) Control and monitoring especially "Take down" of accounts that contain hoax news and hate speech are still centralized (top down from the Police Region and Headquarters), so that both Resort Police and Police Sector cannot initiate quickly and

responsively in order to carry out investigative actions and investigation.

7) Resort Police are still not supported by adequate facilities and infrastructure evenly, especially IT systems that are capable of deterring, terrorism and hoaxes to support the investigation and investigation efforts quickly and responsively, while the Task Force of Cyber troops and patrol are still under the control of the Operational Section of the Resort Police, making it less free to take the initiative and develop tasks to anticipate the spread of news, terrorism and hoaxes more quickly.

8) Socialization carried out by Community Partnership in almost every Resort Police is still on the Real and factual approach, and is not followed by socialization through cyberspace, while the public has been using IT System smartphones on a massive basis, as a result hoax news that is spread through social media platforms is not can be deterred more quickly, in addition to the Community Police Partnership not yet sporadically disseminating "Hotline numbers" to netizens.

9) Hoax news that is found is not only a matter of state, but is also used by people who are not responsible for the students, one example occurred in the city of Cirebon when changing the name of a private university, Gunung Jati University, spread the news that there will be changes the foundation's management became the sole owner, whereas on the contrary the change of name actually optimized the university's brand to be more universal, but the university did not have special technology to counter the news of the hoax, this was confirmed by Agus Dimyati as Vice Rector of Gunung Jati University.

10) The spread of hoax news through social media in West Java has more to do with the presidential election contestation and the 2019 legislative elections, where the intensity of the hoax experienced a sharp increase in relation to the two political events. The results of cyber patrols carried out on hoax content generally originate or are produced by actors outside West Java, while in West Java it is only in the form of sharing by West Java community accounts.

11) Both at the West Java Regional Police and police ranks up to the precincts have been formed cyber troops that actively carry out cyber patrol activities, conduct counter issues and spread performance / narrative narratives, and even take down accounts that spread hoax news. The main activity of the cyber patrol is to surf on various social media to search and find content or posts that are negative. If this kind of content is considered viral and tends to influence the views and attitudes of the public, then counter issue and counter narrative efforts are made as well as by taking the actual news sources and then neutralized together by personnel of cyber troops.

12) Cyber patrol platforms are generally carried out on social media Facebook, Instagram, and Twitter. For patrols in Whatsapp groups, there are no police officers in the ranks. Likewise, sites that spread radical and terrorist content have also not patrolled this platform.

13) Various anticipatory activities carried out in the cyber world are carried out by each function in the territorial unit in accordance with its contributive role as regulated through the Nusantara Task Force in West Java Regional Police. Each content that is done by each function, in accordance with the portion determined in the Special Force of Nusantara, is compiled by the Public Relations function and then uploaded and sold through various official social media accounts of the Kun Fund owned by the Jakarta Police Public Relations function.

14) The creativity of the Resort Police District was also demonstrated by the Blitar District Police by empowering the command center as an information center that was optimized to build a command center link for the communication and information service of the Blitar District Government, so that the synergy of radical news and hoax information was quickly anticipated and resolved. To maintain this synergy the Blitar District Police District routinely conducts group discussion forums (FGD) involving all components of the Blitar Regency Government and community leaders, with the agenda of resolving and clarifying various issues related to social issues including anticipation of hoax and radical news.

15) The main concern felt by East Java Cyber Troops personnel is the risk or legal implications related to their activities in cyberspace using shadow accounts. The average officer is worried if they are actually involved in legal issues as a result of this.

16) The main elements of cyber troops are the Public Relations, Intelligence and Criminal functions. In addition to the police station level, personnel of the cyber troops also consist of personnel of the police station. Each function involved was taken by 5 people, as well as the personnel of each police station were taken by 5 people as personnel of cyber troops. Each cyber troop personnel are asked to create / have at least five accounts in each type of social media. The aim is to simultaneously report negative content on certain social media so that the social media will respond to the report and block or suspend the account. On the other hand, these shadow accounts also function as a means to neutralize issues that will be counter to negative news or content or hoaxes that are already viral.

17) According to local figures in North Sumatra, the issue that became a hoax content has been handled well at the national level, but at the local level this problem has not been taken seriously. This is caused by the turmoil that afflicts the law enforcement circles if those who spread the hoax are religious leaders. There is a very dilemmatic condition for law enforcement. Public intervention strongly influences the intention of law enforcers rather than the intervention of the authorities.

18) Various anticipation activities carried out in the cyber world are carried out by each function in the territorial unit in accordance with its contributive role as regulated through the Nusantara Task Force. Each function performed by each function, in accordance with the portion specified in the Nusantara Task Force, is compiled by the Public Relations function and then uploaded and traded through various official social fund accounts of the Kun Fund owned by the Public Relations function.

19) Anticipatory steps are also carried out by integrating them into conventional Non Commisioner Police Officer of Public partneship activities, such as Door to door Systems, Counseling, and Police Goes to School and seminar activities.

20) Scouting activities are also facilitated by the police to instill the values of anti-radicalism and terrorism, and also to instill the values of love and diversity of the Unitary Republic of Indonesia.

21) Mobile morning activities are carried out by the Partnership function to provide Security and public order appeals. It also includes an understanding of, terrorism and efforts to provide understanding to the public about hoax or Hoax news that is spread through social media and whatsapp groups.

22) The spread of hoax news through social media in Bali has more to do with the presidential and contestation elections in 2019. The intensity of hoaxes tends to increase sharply in connection with these two political events. The results of cyber patrols carried out on hoax content generally originate from or are produced by actors outside Bali, while in Bali it is only in the form of sharing by Balinese accounts.

23) The handling model as developed by the Counter Transnational Organized Crimes (CTOC) task force, which is a task force formed by the Bali Police Chief Inspector General Petrus R Golose, in dealing with cybercrimes is an example and orientation in handling terrorism content, and hoaxes by the ranks of police.

24) Various anticipation activities carried out in the cyber world are carried out by each function in the territorial unit in accordance with its contributive role as regulated through the Nusantara Task Force. Each function performed by each function, in accordance with the portion specified in the Nusantara Task Force, is compiled by the Public Relations function and then uploaded and traded through various official social fund accounts of the Kun Fund owned by the Public Relations function.

25) Anticipatory steps which are also carried out by making Anti Hoax movements or declaration either through joint declarations or banners. Declarations in the cyber world are also carried out by personnel of Non Commisioner Police Officer of Public partneship every day by making video testimonials declaration from various figures and communities which are then sent to the public relations function for uploading to social media or the official territorial unit account.

### 4.4 Influence between Variables

#### 4.4.1 Synergi's Influence, IT Systems, Risk Management on Propaganda indicators

The results of data processed using the SPSS 19 program are shown in table 3 below.

*Table 3. Effects of Synergy, IT Systems, Risk Management on Cyber terrorism and Hoaxes (Propaganda indicators)*

| No<br>. | Variable | Partial | | Simultaneous | |
|---|---|---|---|---|---|
| | | Koef | Sig | Adjusted R Square | Sig |
| 1 | Synergy | -.189 | .007 | - | - |
| 2 | System IT | -.055 | .050 | - | - |
| 3 | Risk Management | -.107 | .049 | - | - |
| 4 | Synergy, System IT, Risk Management | - | - | .969 | .000$^{b}$ |

S*ource: Output SPSS19*

Based on the above table 3, it can be seen that synergi has a negative and significant effect on cyber terrorists and hoaxes with propaganda indicators partially = -0.189, information systems technology =-0,55 and risk management = -0,107, and simultaneously the value of Adjusted R. Square =0.969. The meaning is that if partially and simultaneously the variable is improved, the cyber terrorist and hoax with propaganda indicator will decrease significantly.

### 4.4.2 Effect of Synergi, IT Systems, Risk Management on Agitation indicators

The results of data processing using the SPSS 19 program are shown in table 4 below.

*Table 4. Effects of Synergy, IT Systems, Risk Management on Cyberterrorism and Hoaxes (Agitation indicators)*

| No. | Variable | Partial | | Simultaneous | |
|---|---|---|---|---|---|
| | | Koef | Sig | Adjusted R Square | Sig |
| 1 | Synergy | -.047 | .448 | - | - |
| 2 | System IT | -.042 | .094 | - | - |
| 3 | Risk Management | -.459 | .007 | - | - |
| 4 | Synergy, System IT, Risk Management | - | - | 0,977 | .000<br>b |

*Source: Output SPSS19*

Based on the above table 4, it can be seen that Synergy has a negative and significant effect on cyber terrorists and hoaxes with Agitation indicators partially = -0.47, information systems technology =-0,42 and risk management = -0,459, and simultaneously the value of Adjusted R. Square =0.977. The meaning is that if partially and simultaneously the variable is improved, the cyber terrorist and hoax with Agitation indicator will decrease significantly.

### 4.4.3 Effect of Synergi, IT Systems, Risk Management on Doctrine indicators

The results of data processing using the SPSS 19 program are shown in table 5 below.

Table 5. Effects of Synergy, IT Systems, Risk Management on Cyberterrorism and Hoax Actions (Doctrine indicators)

| No. | Variabel | Partial | | Simultaneous | |
|---|---|---|---|---|---|
| | | Koef | Sig | Adjusted R Square | Sig |
| 1 | Synergy | -.333 | .000 | - | - |
| 2 | System IT | -.206 | .015 | - | - |
| 3 | Risk Management | -.233 | .039 | - | - |
| 4 | Synergy, System IT, Risk Management | - | - | 0,975 | .000$^{b}$ |

*Source: Output SPSS19*

Based on the above table 5, it can be seen that Synergy has a negative and significant effect on cyber terrorists and hoaxes with Doctrine indicators partially = -0.33, information systems technology =-0,206 and risk management = -0,233, and simultaneously the value of Adjusted R. Square =0.975. The meaning is that if partially and simultaneously the variable is improved, the cyber terrorist and hoax with Doctrine indicator will decrease significantly.

### 4.4.4 Effects of Synergy, IT Systems, Risk Management on Jihadist indicators

The results of data processing using the SPSS 19 program are shown in table 6 below.

*Table 6. Effects of Synergy, IT Systems, Risk Management on Cyberterrorism and Hoaxes (Jihadist indicators)*

| No. | Variable | Partial | | Simultaneous | |
|---|---|---|---|---|---|
| | | Koef | Sig | Adjusted R Square | Sig |
| 1 | Synergy | -.137 | .028 | - | - |
| 2 | System IT | -.362 | .080 | - | - |
| 3 | Risk Management | -.064 | .074 | - | - |
| 4 | Synergy, System IT, Risk Management | - | - | 0,983 | .000$^{b}$ |

*Source: Output SPSS19*

Based on the above table 6, it can be seen that Synergy has a negative and significant effect on cyber terrorists and hoaxes with Jihadist indicators partially = -0.137, information systems technology =-0,362 and risk management = -0,064, and simultaneously the value of Adjusted R. Square =0.983. The meaning is that if partially and simultaneously the variable is improved, the cyber terrorist and hoax with Jihadist indicator will decrease significantly, this evidence in line with Banez, Justin D. [8].

### 4.4.5 Discussion

The form and description of cyber terrorism and hoax acts with typology of perpetrators of terrorism consisting of perpetrators with a long-standing ideology and a "long grudging" background on ancestors who experienced excesses of law enforcement carried out by the government. The typology of Hoax that colors the flow of social media in Indonesia consists of; a). Proper Hoax is a hoax with the same title and content and is not based on strong and valid facts and data; b). Hoax titles are hoaxes with incorrect titles and are different from the news content; c). Disguise hoax is news hoax by presenting news / events that are old and not relevant at the moment. Human resource competencies and risk management of cyber troops who carry out cyber patrol have a major role in operating technology, especially in the current 4.0 technology era, the fact that there is a risk management readiness, especially at the Resort Police level many are still not aware and do not understand IT. The loss of space and time limits on the Internet changes many things. The rapid development in the use of internet services eventually led to crime, better known as Cybercrime.

Furthermore, The Influence of Synergy on the Acts of Cyber Terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is negative and significant, meaning that if the police synergy with stakeholders increases, cyber terrorism in the form of propaganda decreases significantly. This is supported by respondents' perceptive data which shows that the implementation of synergy is good around 76-82%. This study agree with Covey [13] also Chin, Anantharaman et al. [10].

While, The Influence of the IT System on the Acts of Cyber Terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is negative and significant, meaning that if the The Indonesian National Polic IT System is good, the cyber terrorism acts in the form of propaganda decrease significantly. This is supported by respondents' perceptive data which shows that the implementation of synergy is good around 58-64%. This study agree with Ineu Rahmawati [22].

While, The Influence of Risk Management on the Acts of Cyber Terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is negative and significant, meaning that The Indonesian National Police's Risk Management is good, then cyber terrorism in the form of propaganda decreases significantly. This is supported by respondents' perceptive data which shows that the implementation of synergy is good around 60-67%. This study agree with Ineu Rahmawati [22], COSO [11], Andersen, T.J. [4].

And Simultaneously the influence of Synergy, IT System, Risk Management, Against the Acts of Cyber terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is negative and significant, meaning that if Synergy, IT System, Risk Management of the National Police are good, then cyber terrorism acts in Jihadist forms decreased significantly. This is supported by respondents' perception data which shows that the implementation of Synergy, IT System, Risk Management, has been good around 58-82%. This study agree with Chin, Anantharaman et al. [10], Ineu Rahmawati [22], COSO [11], Andersen, T.J. [4]..

## 5. CONCLUSION

1) The form and description of cyber terrorism and hoax acts with typology of perpetrators of terrorism consisting of perpetrators with a long-standing ideology and a "long grudging" background, and The typology of Hoax that colors the flow of social media in Indonesia consists of; a). Proper Hoax; b). Hoax titles, c). Disguise hoax , while Human resource competencies and risk management of cyber troops who carry out cyber patrol have a major role in operating technology, especially in the current 4.0 technology era, the fact that there is a risk management readiness, especially at the Resort Police level many are still not aware and do not understand IT. The loss of space and time limits on the Internet changes many things. The rapid development in the use of internet services eventually led to crime, better known as Cybercrime.

2) Partially, the variable Synergy has negatively and significantly influence on Acts of Cyber Terrorism and Hoax , where respondents agree and strongly agree around 76% -82%.
3) Partially, the variable IT System has negatively and significantly influence on Acts of Cyber Terrorism and Hoax where respondents agree and strongly agree around only 58 - 64%.
4) Partially, the variable Risk Management has negatively and significantly influence on Acts of Cyber Terrorism and Hoax , whree A qualified Risk Management is still considered moderate with a score of 60% - 67%.
5) Simultaneously the influence of Synergy, IT System, Risk Management toward the Acts of Cyber terrorism and Hoax with indicators of propaganda, agitation, doctrine, jihadists is also negatively and significantly, meaning that if Synergy, IT System, Risk Management of the National Police are good, then cyber terrorism acts decreased significantly. This is supported by respondents' perception data which shows that the implementation of Synergy, IT System, Risk Management, has been good and adjsuted R Square equal 98,3%. As a major finding that hoax typology is very varied and public perceptions about synergy, IT systems and risk management implemented by the Indonesian Police are good enough to significantly influence toward Cyber Terrorism and the spread hoax news. This study agree with Chin, Anantharaman et al. [10], Ineu Rahmawati [22], COSO [11], Andersen, T.J. [4].

## 6. IMPLICATIONS

1) Resort Police should improve synergy with the Ministry of Communication and Information and the Private, Academic, Media, Regency, Municipality in building information systems that can detect and anticipate the dissemination of hoax news earlier.
2) Anticipation of radicalism and news of hoaxes requires modern technological facilities and infrastructure, ideally these facilities and infrastructure are available at the Resort Police and Police sector levels, so that prevention of radicalism and news of hoaxes can be prevented early on at the lowest level, but in reality the facilities and infrastructure cyber infrastructure is only available at the Police Region level, besides that the main authority in counteracting hoax news and radicalism lies with the Police Region. While the issue of terrorism is directly handled centrally by the National Police Headquarters *“Detasement 88”*. The handling of such a model is felt to be less than optimal given the escalation of hoaxes and radicalism spread more quickly.
3) The Resort Police should have a command center connected to the criminal justice system (CJS) and the Regional Government Communication Center, so that the spread of radicalism and hoax news is early and quickly anticipated and dealt with quickly. Cyber issues at the Resort Police level are not structurally and centrally organized, with a room that can monitor the development of hoax news and radicalism in detail at any time that can directly map and analyze centrally, while monitoring work still relies on the ability of individual personnel to handle and operate news hoaxes and radicalism through a limited laptop or PC which can slow down the anticipation of radicalism handling and hoax reporting.
4) The National Police needs to propose amendments to the ITE Law to control the entry and exit gates of content and news, terrorism and hoaxes which are relatively numerous with a single (*"Kanal”*) system to facilitate cyber troops and cyber patrol to quickly and optimally anticipate and detect opportunities.
5) It is necessary to implement risk management in order to protect and provide legal guarantees for the main concerns felt by Cyber Troops personnel relating to their activities in cyberspace using shadow accounts, and in the recruitment process of The Indonesian National police personnel, so that Talent Scouting is conducted for candidates The Indonesian National Police personnel who are sourced from the public who have expertise in the field of Information and Technology (IT), so that they can be placed in the “Nusantara Task Force” or in Public Relations at each Resort Police.
6) The Indonesian National Police should adopt the Counter Transnational Organized crimes (CTOC) task force, which is a task

force formed by the Bali Police Chief Inspector General Petrus R Golose, in dealing with cybercrimes that can be used as an example and orientation for handling terrorist content, and a hoax by local police ranks based on local wisdom in each region.

## REFERENCES :

[1] Allison Shorten and Joanna Smith (2017), Mixed methods research: expanding the evidence base, Evid Based NursJuly 2017, volume 20, number 3, http://dx.doi.org/10.1136/eb-2017-102699

[2] Abdul Karim and Firdaus Wajdi (2019), Propaganda and Da'wah in Digital Era (A Case of Hoax Cyber- Bullying Against Ulama), Karsa: Journal of Social and Islamic Culture Vol. 27 No. 1, June 2019, pp. 171-202. file:///C:/Users/Asus/Downloads/1921-5412-1-PB.pdf

[3] Andriana Deni. (2010). Triangulasi dan Keabsahan Data dalam Penelitian Goyang Karawang. http://www.goyangkarawang.com/2010/02/25. Accessed on 16 January 2019.

[4] Andersen, T.J. (2008). "The Performance Relationship of Effective Risk Management, Exploring the firm specific investment retaionale, long range planning, Vol. 41. No. 2

[5] Ahmad, Rabiah and Yunos Zahri, (2012), A Dynamic cyber terorism frame work, International Journal of Computer Science and Information Security; Pittsburgh, Feb 2012

[6] Astuti, Sri Ayu (2015), Law Enforcement of Cyber Terorism in Indonesia Vol. 2 (2), December 2015, http://ojs.umsida. ac.id/ index.php/rechtsidee

[7] Agusta Ivanovich. (2009). Teknik Pengumpulan dan Analisis Data Kualitatif. http://www.ivanagusta.files.wordpress.com/2009. Accessed on 11 Januari 2019.

[8] Banez, Justin D. (2010). The Internet and The Homegrown Jihadist Terrorism: Assessing U.S. Detection Techniques (Thesis, Naval Postgraduate School, California). Retrieved from https://www.hsdl.org/?view&did=11245

[9] Bambang A.S, Idealisa Fitriana (2017), Cyber terrorism: Suatu tantangan komunikasi asimetris Bagi ketahanan Nasional. Jurnal Komunisasi, Vol 2,No.1 . file:///C:/Users/Asus/Downloads/12-43-1-PB%20%281%29.pdf

[10] Chin, S. T. S., R. N. Anantharaman, et al. (2011). "The Roles of Emotional Intelligence and Spiritual Intelligence at the Workplace." Journal of Human Resources Management Research 2011: 1-9

[11] COSO, (2004). Enterprise risk management–integrated framework. Committee of Sponsoring Organizations, www.coso.org/Publications/ERM/COSO_ERM_ Executive Summary.pdf.

[12] Collin, B. L. Collin (1996), "The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge," in 1 1th Annual International Symposium CriminalJustice Issues, 1996, vol. 93, no. 4.d

[13] Covey, Stephen R., (1989), The 7 Habits Of Highly Efektif People, (Newyork: Simon & Schuster.

[14] Christiany Judhita, (2018). "Interaksi Komunikasi Hoax di Media Sosial serta Antisipasinya Hoax Communication Interactivity in Social Media and Anticipation" *Jurnal Pekommas,* Vol. 3 No. 1, April 2018: 31-44. Jakarta: Puslitbang Aplikasi Informatika dan Informasi Komunikasi Publik Kementerian Komunikasi dan Informatika RI.

[15] Dedi Rianto Rahadi (2017), Perilaku Pengguna Dan Informasi Hoax Di Media Sosial , Jurnal Manajemen dan Kewirausahaan, Vol.5 no.1, file:///C:/Users/Asus/Downloads/1342-3734-1-PB.pdf

[16] Denning Dorothy. E. (2000), "Cyberterrorism," Testimony given to the House Armed Services Committee Special Oversight Panel on Terrorism, 2000

[17] Dista Amalia Arifah, (2011). "Kasus *Cybercrime* Di Indonesia Indonesia's *Cybercrime Case" Jurnal Bisnis dan Ekonomi (JBE),* September (2011), Hal. 185 – 195 Vol. 18, No. 2. Semarang: UNISULA.

[18] Eska Nia Sarinastiti dan Nabilla Kusuma Vardhani, (2018). "Internet Dan Terorisme: Menguatnya Aksi Global Cyber-Terrorism Melalui New Media". *Jurnal Gama Societa,* Vol. 1 No. 1, Januari 2018, 40 – 52. Yogjakarta: Universitas Gajah Mada.

[19] Galamas, Francisco, (2015), Terorisme in Indonesia : an Overview, The Militant Groups Of Radical Ideology And Violent Nature Series Area: Indian Subcontinent And Southeast Asia, Research Papers 04/2015

[20] Ghozali, Imam. (2013). Aplikasi Analisis Multivariate Dengan Program SPSS. Semarang : Badan Penerbit Universitas Diponegoro

[21] Harley, D., (2008). *Common Hoaxes and Chain Letters*. San Diego: ESET, LLC

[22] Ineu Rahmawati (2017), Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense The Analysis Of Cyber Crime Threat Risk Management To Increase Cyber DefenseJurnal Pertahanan & Bela Negara | Agustus 2017, Volume 7 Nomor 2. http://jurnal.idu.ac.id/index.php/JPBH/article/viewFile/179/84

[23] Ivancevich, John M., Konopaske and Matterson (2008): Organizatonal Behavior and Management. New York: The McGraw Hill, Inc, 2008

[24] J.A. Scholte, (2000), Globalization: A Critical Introduction, (London: Palgrave, 2000),http://aditi.du.ac.in/uploads/econtent/Globalization-Second-Edition-A-Critical-Introduction-.pdf

[25] National Police Agency of Japan (2018), https://www.npa.go.jp/ english/Police_of_Japan/Police_of_Japan_2018_full_text.pdf

[26] O'Brien and Marakas. (2010). Management Information System: Managing Informastion Technology In The Bussiness Enterprise. 15th Ed. New York: McGraw-Hill

[27] P.N. Howard and M.R Parks, (2012), *American Behavioral Scientist*, Vol. 45 No. 3, November 2001 383-404

[28] Respati, S. , (2017), Mengapa Banyak Orang Mudah Percaya Berita "Hoax"? Kompas.com. Retrieved from http://nasional.kompas.com/read/2017/01/23/18181951/mengapa.banyak.orang.mudah.percaya.berita.hoax

[29] Seib, P. & Janbek, D.M. (2011). Global Terrorism and New Media: The post-Al Qaeda generation. New York: Routledge Taylor & Francis Group

[30] Turban, Efraim, R. Kelly Rainer, Jr, and Richard E. Potter. (2005). Introduction To Informa tion Technology. 3rd edition. John Wiley & Sons, United States

[31] Fitria Chusna Farisa (2019),"Cyber Crime Polri: Ada 1.005 Kasus Penyebaran Hoaks Selama Pemilu 2019", accessed on 29 August 2019https://nasional.kompas.com/read/2019/08/20/16552311/cyber-crime-polri-ada-1005-kasus-penyebaran-hoaks-selama-pemilu-2019

[32] Tito Karnavian (2017), Ada 31 Kasus Terorisme di Indonesia Selama 2 Tahun https://www.suara.com/news/2017/07/17/144604/ada-31-kasus-terorisme-di/ accessed on 29 January 2019