ISSN 2303-0089
e-ISSN 2656-9949

DINAMIKA GOVERNANCE
JURNAL ILMU ADMINISTRASI NEGARA
DOI: http://ejournal.upnjatim.ac.id/index.php/jdg/article/view/4352

CYBERSECURITY STRATEGIES AND MEASURES HOAX IN THE DIGITALIZATION ERA

Mohammad Fadil Imran[1]
Sekolah Tinggi Ilmu Kepolisian, Jakarta
mfadilimran@stik-ptik.ac.id

ARTICLE INFORMATION

Article history:
Received date: 12 November 2023
Revised date: 15 November 2023
Accepted date: 24 Januari 2024

ABSTRACT

With the presence of growing digitalization, people are able to obtain various conveniences in many things efficiently and optimally, such as storage, security and increasing the resolution of both images and sound to the maximum. In general, almost all areas of human life that require the use of technological processes are based on digitalization. The product of this digitalization technology is internet-based information and communication technology. Considering that Indonesia has an increasing number of internet users, Indonesia has reached 213 million users out of a total of 276.4 million people as of January 2023, or it can be estimated that 77%. This is of course balanced with cyber security to protect the data held by the state for its citizens. However, with this development, the Indonesian state is still not strong enough in terms of cyber security and is often subject to attacks or threats and even the emergence of hoax information that cannot be resolved and is not proven to be true. With this, there needs to be efforts and strategies in strengthening cyber security in preventing and controlling cyber attacks on cyber security in a country, including strengthening capacity building, forming and enacting laws specifically regarding cyber crime, improving the human resources sector and carrying out cooperation both on a national and national scale. Internationally to overcome emerging cyber attacks and prevent the spread of hoaxes as early as possible.

Keywords: *Cyber security, security strategy, countering Hoaxes, Digitalization*

ABSTRAK

Dengan hadirnya digitalisasi yang semakin berkembang, masyarakat bisa memperoleh berbagai kemudahan dalam banyak hal secara efisien dan optimal, seperti penyimpanan, keamanan dan peningkatan resolusi baik gambar maupun suara secara maksimal. Secara umum, hampir seluruh bidang kehidupan manusia yang memerlukan pemanfaatan proses teknologi berbasis digitalisasi. Produk dari teknologi digitalisasi ini adalah teknologi informasi dan komunikasi berbasis internet. Mengingat Indonesia memiliki jumlah pengguna internet yang semakin meningkat, Indonesia telah mencapai 213 juta pengguna dari total 276,4 juta jiwa per Januari 2023 atau diperkirakan sebesar 77%. Hal ini tentunya diimbangi dengan keamanan siber untuk melindungi data yang dimiliki negara bagi warganya. Namun dengan perkembangan tersebut, negara Indonesia masih belum cukup kuat dalam hal keamanan siber dan sering menjadi sasaran serangan atau ancaman bahkan munculnya informasi hoax yang tidak dapat diselesaikan dan tidak terbukti kebenarannya. Dengan hal tersebut, perlu adanya upaya dan strategi penguatan keamanan siber dalam mencegah dan mengendalikan serangan siber terhadap keamanan siber di suatu negara, termasuk memperkuat peningkatan kapasitas, membentuk dan menetapkan undang-undang khusus mengenai kejahatan siber, meningkatkan sektor sumber daya manusia dan melakukan kerja sama. baik dalam skala nasional maupun nasional. Secara internasional untuk mengatasi munculnya serangan siber dan mencegah penyebaran hoax sedini mungkin.

Kata Kunci: Keamanan siber, strategi keamanan, penanggulangan Hoax, Digitalisasi

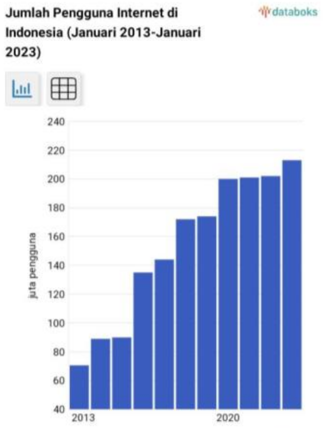
INTRODUCTION

The existence of information becomes an inseparable thing in the change and development of society in carrying out any form of activity that can influence the different conditions and situations in an environment. With the advancement of technology, communication as a messenger has begun to use a variety of new media or technology equipment as a replacement for a face-to-face model that can generally make it easier for the public to receive and disseminate forms of information that are private or public. The shift in the social communication model has changed the process of dissemination of information from analog communication to digital communication. There is a change that makes it easier for society in particular to save time and energy when communicating because it has switched to a mobile phone or computer communication device to transmit or interconnect information to an individual or group called digitization-based information. Indirectly, the existence of this digitization has become one of the models that society continues to pursue to obtain all forms of information that are unlimited and can be disseminated more widely with technological advances that can be used by anyone.

Digitalization has become a form of media transfer in the fields of communication and public information, such as media, audio, images, and video. In digitalization, all information consisting of text, sound, images, and multimedia is stored electronically. In the presence of growing digitalization, people are able to obtain a variety of facilities for many things efficiently and optimally, such as storage, security, and enhancing the resolution of both images and sounds to the maximum. Generally speaking, almost every area of human life that is needed uses technology processes based on digitization. Essential data has become one of the key points in the shift of the digitization process to use in various fields such as telecommunications, broadcasting, and government services. Generally speaking, digitization brings a change in impact for people to realize and follow the importance of the presence of technology along with rapid development so that people can access all information, services, communications, and knowledge easily and quickly on a wide scale. This makes the role of digitalization capable of supporting and supplementing community activities with technology-based systems.

As a democracy, the existence of the era of digitalization in Indonesia is characterized by the availability of people who have the freedom to choose, express, or express their opinions widely through the use of devices based on information and communication technologies. The existence of an era of digitalization in a country can make it easier to interact, communicate, and build a standard governance system based on the principles of accountability and transparency. But on the other hand, the advances of the era of digitalization can have negative implications, including the use of social media and the significance of smartphones in the social environment.

Becoming a country with a densely occupied rate and becoming one of the largest countries in Internet use in the world. Through the use of the Internet, the presence and use of social media are increasing and developing in Indonesia, but they are often abused by the public in committing crimes or by the elite, who exploit political or business interests manipulatively. This is happening as the growing number of Internet users in the Indonesian country has reached 213 million out of a total of 276.4 million by January 2023, or an estimated 77 percent. (Databoks KOMINFO dan Siber Kreasi Tahun 2023). Here's a diagram of Indoesian Internet users from 2013–2023:



According to a report by We Are Sicial, supported by KOMINFO and Siber Kreasi, Internet usage from 2013 to 2023 continues to increase. The country's highest internet usage in 2023 reached 213 million users out of 276.4 million Indonesians. By 2024, this will be one of the pillars of society and the nation as it enters the political year. The widespread use and public reach of technology is one of social media's increasingly obstinate uses by political elites that are exploited to build comprehensive communication to increase interest in winning the year's political contest.

The negative implications of the use of social media by smart phone devices can cause the occurrence of an increasing spread of hoaxes because, in general, society is not aware of and does not have sufficient knowledge to ensure accurate and correct information from circulating information. According to Suvei Master, the overall spread of hoaxes stems from the use of social media, which reached 92.4% with a wide range of content that is infringing and does not have the values and ethics of society. According to the State Intelligence Agency, it also estimates that 60% of all content on social media indicates a hoax.

Therefore, the prevention of social hoaxes is essential because it enables the division of society and the state, one of which is to strengthen cyber security or cyber protection to maintain and protect the massive cyber safety of mobile devices, computers, electronic systems, networks, and data privacy from various kinds of malicious attacks. Cybersecurity is a measure taken to protect information circulating on social media that generally arises from the existence of daily use of the Internet.

According to Hasyim Gautama in general the debate on the strategy of strengthening cybersecurity in Indonesia between the weak knowledge of the understanding of the state maintenance of cyber security that strongly requires restrictions on the use of remote services and requires the existence of secure systems, there is and exists the legal body against the prevention of cyberspace attacks, patterns of attacks from cyber crime too fast and difficult to solve, limited in implementing the institutional framework of cybersecurity at the national level, awareness of the threat of international cyber attacks is still low at risk of collapse of important infrastructure in a country, the minimum domestic industry to reduce and build hardware on information technology is one way in strengthening or weakening cyber safety.

Therefore, Indonesia is in great need of a strategy and cyber security effort to deal with information or hoax news in society as digital developments continue to spread in the midst of society. One of the drivers of this effort is to manage cyber security by understanding the scope of cyber vulnerability, and there is a solution that is found because it is possible that without the proper efforts to strengthen cyber protection risks, problems, conflicts, or threats will occur in the future in society or the country.

LITERATURE REVIEW

A. Cyber Security

Cyberspace, or what we call cyberattacks, is a logical consequence of the widespread development of information technology. The forms of cyber attacks can be identified in various ways, such as cybercrime or crimecyber, botnets, attacks on financial-related agencies, the spread of multi-purpose malware, cyber activities funded by the state or government, and public activity. (Cynthia Rahmawati, 2019). Generally speaking, the form of the trend related to the component of cyberspace is to be the main channel for carrying out various actions in cybersecurity.

The definition of cyber security itself is an activity or attempt to carry out the protection, prevention, and security of classified telematics resources to prevent the occurrence of crime in the cyber world. As for the basic elements of cyber security, such as security policy documents, information infrastructure, perimeter defense, network monitoring systems, information systems and event management, network security assessment, human resources, and awareness of location, (Human Resource and Security Awareness) Information systems are also called hardening, which means an attempt to strengthen the security of the information system infrastructure, in particular computer devices or others, by strengthening various sides such as the network, computer device systems, and the closure of ports and firewalls. (Rahmani, Aziz, 2019). General scara based on human resources can be grouped into three large groups that are used to cyber security practices among security analysts, forensics specialists, and hackers.

Cybersecurity has the function and role of finding, repairing, and minimizing the impact of various threats or cyber attacks and all activities related to security threats on all components or instruments of cyber systems, such as hardware, software, data, information, and critical infrastructure. (L. Siagian, 2017). There are different perspectives and terminologies regarding the concept of cybersecurity because cyberspace is a virtual space that is built and created through the form of collaboration between human beings and technology (information and communication technology). (Dista Amalia Arifah, 2011).

So cybersecurity, with its development, is widening into the technological realm and can generally pose a threat to national prosperity. With the advancement of modern information and communication technology, the state is adapting directly to the concept of cybersecurity. This concept of security has become one of its own parts that has its own territory, so that the state can maintain and protect the cyber security that is circulating in a country. This is in line with the emergence of cyber attacks that not only attack public agencies but can also attack government agencies in a nation. Cybersecurity addresses information security issues for governments, organizations, and individual affairs connected with technology, specifically Internet technology. (I. A. Afandi, A. Kusyanti, and N. H. Wardani, 2017). Cybersecurity cannot be extracted too far from its scope and socio-cultural environment.

B. Security Strategy

The terms information security and cybersecurity are two different concepts, but they have a similar understanding of a particular context when connected with the protection of assets against surveillance activities of the industrial and economic sectors, the fight against terrorism or economic crime, and the prosecution of contents that infringe or deviate (Ghernaouti, Solange, 2013). Cybersecurity has coverage related to computer surveillance, supervision, and very high control over fundamental rights. While information security concerns more comprehensive issues such as national sovereignty, national security, protection of critical infrastructure, security of certain assets, protection of private and public data, and so on, (Dewi Triwahyuni, Tine Agustin Wulandari, 2016).

The development of security within a country is accelerating, involving a wide range of central sectors in both the community and the country. The notion of independence is becoming wider and deeper as a country releases its limitations on information technology, which can create a relationship of conflict or cooperation between countries but extends to guarantees of security for the whole of society. According to Arnold Wolfers in Perwita & Yani, the definition of security is "security, in any objective sense, measures the absence of threats to acquired values and, in a subjective sense, the lack of fear that such values will be attacked." According to John P. Lovell, a strategy is a framework that has alternatives and decisions that have been planned in a particular situation or circumstance with the aim not only to generate profits but the success of benefits in general. Another definition of strategy is a way to promote the achievement of a goal by using the power that one possesses, including military power. (Eko Budi, Dwi Wira, Ardian Infantono, 2021).

According to Arnold Global cyber security is composed of five areas of work including legal certainty (Laws on cyber criminalization), technical standards and procedural measures (end users and by taking approach to service providers and software), institutional structure (distribution of tasks according to the organizational structure occupied to avoid intersection of posts or tasks), capacity building and user knowledge education (socialization and direct communication of various threats of cyber crime intensely), international cooperation (relationship concerning work related to attempts to deter attacks or cyber threats), regular examination of international security often with significant developments. (Perwita & Yani, 2005: 119).

C. Digitalization

Digitalization becomes a form of media transfer in the field of communication and public information, such as small media, audio, images, or videos. Digitalization stores all information consisting of text, voice, images, or multimedia on an electronic basis. In the presence of growing digitalization, people are able to access a variety of things with ease in an efficient and optimal way, such as storage, security, and enhancing the resolution of both images and sounds to the maximum. Generally speaking, almost every area of human life that is needed uses technology processes based on digitization. Essential data has become one of the key points in the shift of the digitization process to use in various fields such as telecommunications, broadcasting, and government services. Generally speaking, digitization brings a change in impact for people to realize and follow the importance of the presence of technology along with rapid development so that people can access all information, services, communications, and knowledge easily and quickly on a wide scale. This makes the role of digitalization capable of supporting and supplementing community activities with technology-based systems.

Through the digitalization model, the broadcaster has the right to obtain, communicate, and receive information without limit, including the right to information and communication with the government. (Nurjanah & Iswanto, 2021). The development of technology in the field of communications and information has become one of the steps that must be followed wisely by any individual or group that can be used as a balancer of life in an increasingly urban era. With the all-digitalization-based model, system change and usage are applied gradually by connecting more flexible networks across the various components as their supporting functions. (Zutiasari et al., 2020).

The use of information technology can be seen from the presence of certainty of information, clarity of the content, information framework, useful information parameters, i.e., the quantity of information, the content of the information, information structure, the use of words and signs that have meaning in information, a time limit of validity of information that can be utilized to the maximum in a situation, and conditions adapted. Information religions can be in the form of news manuscripts or images that contain meaningful information in an institution that is used as an organizational archive. (Mindarti et al., 2020). Generally, information is derived from the processing of various data that can be found scientifically or naturally. The data usually contains a variety of events as well as information that effectively characterizes the development of society's life that can happen now and in the past according to the events that occurred. (Hutahaean, 2015). The development of information and communication technology has become one of the developments that have a great influence on the ecosystem of life of people, along with a variety of activities carried out in various sectors. (Purwanto, E.A., and Sulistyastuti, 2001).

D. Dealing with hoaxes

The term hoax was known and popularized by academics by Curtis Mac Dougall in 1958. The definition of a hoax is a combination of uncertainty and inaccuracies that are planned and modified as if they were factual and true information. From the beginning, the term hoax refers to something that has no value in terms of truth and invalid information that can be accepted as a fact. According to John Hartley, hoak always tends to have the characteristics of a chain message to everyone (Aprinus Salam, 2018). Second, usually, a hoax is not accompanied by valid event data and brief impressive information that cannot diversify its truth (Aprius Salam, 2018). Third, information that is a hoax does not have a deadline for the information delivered; fourth, there is no credible organization related to widely disseminated information. (Aprinus Salam, 2018). Of the four characteristics, they are generally still relevant and often found in everyday life, although over time the spread of hoaxes has evolved in a variety of ways, with the appearance of forms, formats, and false information more developed than ever with Internet-based social media as the medium of transmission.

Prevention of hoaxes through social media is constantly undermined by crimes against private interests, so there needs to be a national guide that has the ability to detect them as soon as possible and provide early prevention (Kombes Pol Chaerul Yani, 2019). Not only that, the components and instruments of the nation have a consciousness and a firm belief in the ideological basis of nationalism and nationalism towards the common understanding of the dissemination of information in accordance with its truth and reality in cybersecurity in society. (Sutarso, 2017). There are several theories to be able to identify and analyze related to the still widespread spread of hoaxes and fake news in the country of Indonesia. There are three theories that can explain Indonesian challenges in the face of hoax attacks circulating in society: confirmation bias, prospect theory, and the bandwagon effect. Nickerson's Bias is a theory that says an individual often believes and justifies information presented before (Xinyi Zhou, 2018). The Prospects theory, proposed by Kahneman and Tversky, is the theory that everyone makes decisions based on the information gained without comparing the impact that will occur in the future. (Xinyi Zhou, 2018).

METHODS

A literature review is a description of the theory, findings, and other research materials obtained from the reference material to be used as a research foundation in drawing up the framework of thought for the formulation of the problem studied. Starting from the phase of summarizing, making analysis, and conducting a critical and in-depth synthesis of previous literature. The literature review requires the process of evaluating the quality of the new findings of a scientific paper, one of which is on the strategy and strengthening of cyber security in the hoax embezzlement era of globalization.

RESULTS AND DISCUSSION

The development of the world of information and communication technology is constantly changing at all times. The use of technology is becoming easier with the emergence of various communications and information services for both domestic and national purposes. The presence of technology in one country becomes a challenge of its own considering the use of new technology to be abused by certain people, one of which is the spread of hoaxes. In order to strengthen cyber security in a country as one of the efforts in shaping a national strategy for combating hoaxes in the era of digitalization, there are various alternatives that need to be done, including:

1. Capacity building

A nation's awareness of cybersecurity requires a program of training and expertise-building on cybercrime conducted by a world-class team of professionals such as the Cyber Defense Operation Centre. Building on human resources cybersecurity knowledge as an alternative step in improving understanding and suppressing the emergence of cybercrime. Organize and manage a system-based defense system comprehensively by conducting mature initial preparations that collaborate in shaping a synergy policy with various elements of the state and society, such as cyber defense and cyber security. The existence of this synergy is indirectly capable of forming a network of communication, coordination, networking, and technical cooperation among cyber security communities in the early prevention of various risks and threats of cyber attacks to strengthen national security and defense.

Accelerating the approval of legislation on cybersecurity is essential as a legal basis for action. The existence of the law is decisive for technological development and a driving force in the implementation of a comprehensive national cybersecurity strategy. Digital transformation becomes a layered solution to cyber security and one that is needed to coordinate cyber safety strategies at the national level. The first layer starts with a working unit of both an information technology team and a business team that has the ability to design solutions and provide positive experience motivation. The second layer is a risk management and compliance team with a renewable, comprehensive cyber security capability. In the third layer, there is an audit team as the body of control and supervision related to the preparedness and maturity of cyber security carried out. Given the importance of cyber security, there is an urgent need to strengthen the agencies responsible for carrying out coordination efforts when necessary, with the full support of all parties involved. Thus, cybercrime, one of which is the spread of hoaxes, can be identified at the outset without the risk of the impact concerned.

2. Creation of a special law on cybercrime

The absence of a legal basis for cybersecurity will have an impact on the institutions or agencies carrying out cyber security practices professionally. Indirectly speaking, the absence of regulation means that no one wants to be held accountable for the cyberattacks that are emerging in society. The plan to enact the Cybersecurity Act has not yet been passed and has not been issued to the public, which means that the legislation in force in the field of information technology does not cover cybercrime, so the presence of cybercrime becomes a serious issue for the security and integrity of the nation.

The cybersecurity regulations contain the rule of law for all criminal acts in the field of information and communications technology, criminal offenses relating to the confidentiality, integrity, and availability of data or computer systems or electronic systems, guidelines for financing, the law of events governing the procedures of investigation and investigation in the area of information and communications technology, including the search and seizure of digital evidence tools, and international cooperation in dealing with cybercrime. Having clear laws will make it easier to tackle all forms of cybercrime, including the spread of hoaxes in society.

3. Increased human resources

The main component and objective of the advancement of information and communication technologies is human resources. Human resources have become an indispensable element in ensuring that cyber security is in line with established policies. Improvements to the knowledge and skills grid must be developed at all times to support the change in the circumstances of security needs. Human resources can help cyber security through recruitment programs, training, and building according to the needs and conditions that have been established. In a cybersecurity system, humans become one of the weakest components and often make mistakes in something.

In the management of human resources, technology, as well as research and development (research and development) for strengthening cyber security, the government, in this regard, the Ministry of Education, Culture, Research, and Technology, in cooperation with BSSN and the Department of Communications and Informatics, should undertake a breakthrough effort to educate and recruit information technology security professionals who have the integrity and inviolable ethics to support development and run cybersecurity. It is an attempt to pursue a strategy to strengthen cyber security against the spread of hoaxes in the growing digital age of society. So we can stop the untrue and inaccurate information that continues to spread among the people.

4. National and international cooperation

The issue of cybersecurity is so comprehensive that it requires multi-dimensional approaches. It needs to be done to create improvements to cyber security governance and the implementation of a principle with the various stakeholders involved. It becomes one that is needed on a national scale to be able to build a network of collaboration between different sectors ranging from the private sector, academia, government, and civil society, and problem-solving issues related to cyber security will continue to be one dimension and incomplete. There is a need for an inclusive mechanism that can validate decisions as well as be reflective and responsive to the national interests and populations affected.

International cooperation can be carried out both bilaterally between the two countries as well as regionally and internationally and is one of the strategies for developing and reducing the capacity of human resources capabilities to components or instruments of cyber security, starting with infrastructure, means, and supplies that conform to procedural standards. Increased cooperation in information technology and cybersecurity is also expected to open up opportunities for the development of new media industries related to information technology in Indonesia as part of the national strategic industry development and as an effort to counter the spread of hoaxes in the era of digitalization.

CONCLUSION

A strategy to strengthen cybersecurity in an effort to counter the spread of digital hoaxes is essential. This is very important to be done as the use of information and communication technology through the Internet is increasingly widespread in the country of Indonesia. It can have a positive impact and also a negative impact, depending on the purpose for which the user is running. Therefore, there is a need for cybersecurity that must be enhanced and tightened by the state to prevent the occurrence of threats and cyberattacks that can harm society and the country. Efforts and strategies that can be undertaken to create cybersecurity strengthening in the country include strengthening capacity building, establishing and enforcing a special cyber criminal law, enhancing the human resources sector, and cooperating both nationally and internationally to tackle emerging cyber attacks and halt the spread of hoaxes as soon as possible.

BIBLIOGRAPHY

Aprinus Salam. (2018). “The Hoax Phenomenon in Indonesian Society: Observing Anti-Diversity Memes since 2014”, Humaniora, Vol. 30, No. 3, (2018), hal.318

Cynthia Rahmawati. (2019). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU) Vol. 1, No.1, 25 September 2019, hlm. 299~306 ISSN 2685-8991

Dewi Triwahyuni, Tine Agustin Wulandari. (2016). Strategi Keamanan Cyber Amerika Serikat. Jurnal Ilmu Politik dan Komunikasi Volume VI No. 1 / Juni 2016

Dista Amalia Arifah. (2011). “KASUS CYBERCRIME DI INDONESIA Indonesia’s Cybercrime Case,” J. Bisnis dan Ekon., vol. 18, no. 2, pp. 185–195, 2011.

Eko Budi, Dwi Wira, Ardian Infantono. (2021). Strategi Pengutan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesiap-ISSN 2086-5805 Akademi Angkatan Udara | Yogyakarta, 24-25 November 2021 e-ISSN 2808-2540 Volume 3, Tahun 2021, hlm. 223-234 DOI:10.54706/senastindo.v3.2021.141

Ghernaouti, Solange. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press.

Hutahaean, J. (2015). Konsep Sistem Informasi. Ed.1, Cet.1. Yogyakarta: Deepublish, ISBN 978-602-280-368-3. hal.124

I. A. Afandi, A. Kusyanti, and N. H. Wardani. (2017). “Analisis Hubungan Kesadaran Keamanan, Privasi Informasi , Perilaku Keamanan Pada Para Pengguna Media Sosial Line,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 9, pp. 783–792, 2017.

Kombes Pol Chaerul Yani. (2019). Pencegahan Hoax di Media Sosial Guna Memelihara Harmoni Sosial. Jurnal Kajian Lemhanas RI, Edisi 40, Desember 2019

L. Siagian, A. Budiarto, P. Strategi, P. Udara, and U. Pertahanan. (2017). “The Role of Cyber Security in Overcome Negative Contents To,” pp. 1–18, 2017.

Mindarti, L. I., Saleh, C., & Galih, A. P. (2020). Pemberdayaan Pelayanan dan Tata Kelola Kearsipan di Kelurahan Merjosari Kota Malang. J-Dinamika: Jurnal Pengabdian Masyarakat, 5(1), 76–82. https://doi.org/10.25047/j-dinamika.v5i1.1390

Nurjanah, A., & Iswanto, I. (2021). Digitalisasi Kelembagaan Pedukuhan Melalui Sistem Informasi Berbasis IT di Dusun Nengahan, Bantul, DIY. Warta LPM, 24(4), 626–635. https://journals.ums.ac.id/index.php/warta/article/view/13559

Perwita, Anak Agung Banyu & Yani, Yanyan A. (2005). Pengantar Ilmu Hubungan Internasional. Bandung: Rosdakarya

Pratiwi Utami. (2018). “Hoax in Modern Politics: The Meaning of Hoax in Indonesian Politics and Democracy”, JurnalIlmu SosialdanIlmu Politik, Vol. 22, No. 2, hal.88

Purwanto, E.A dan Sulistyastuti. (2001). Implementasi Kebijakan Publik: Konsep dan Aplikasinya di Indonesia. Yogyakarta : Gava Media.

Rahmani, Aziz. (2019). Information Warfare and Cyber Security. Materi Sekolah Keamanan Nasional, Universitas Bhayangkara Jakarta, Puskamnas Ubhara Jaya, 3 Januari 2019.

Sutarso, Jokoet.Al. (2017). “Literasi Media Sosial dalam Merangkai Keberagaman dalam Harmoni Budaya Nasional” dalam Manajemen Image Kebhinekaan Indonesia. Yogyakarta: BukuLitera.

Xinyi Zhou. (2018). “Fake News: A Survey of Research, Detection Methods, and Opportunities”, ACMComput. Surv. Vol. 1, No. 1, hal.5

Zutiasari, I., Saputri, S. E., Yuvita, L. F., Hotimah, H., Assegaff, M. F., & Malang, U. N. (2020). Sistem Aplikasi Tata Kelola Administrasi (SIPATAS) dalam Peningkatan Pelayanan Prima Administrasi Desa. Jurnal Karinov, 3(3), 140–146