Research Article

Prospects for Digitalization of ASEAN Smart Cities Network Securitization: Case Studies Indonesia

Laode Muhammad Fathun[1]
UPN "Veteran" Jakarta
laodemuhammadfathun@upnvj.ac.id

Abstract

This paper aims to explain the opportunities and challenges of securitization in the digitization of ASCN. This paper uses qualitative methods with case study methods and uses library review data collection techniques. The results found that the digitalization of ASCN is a form of ASEAN's commitment to innovate and digital transformation of the government, society, and the business world. ASCN is a concrete form of public service governance to create connections and integration between cities in ASEAN so that they can collaborate and synergize. However, from this cooperation, several opportunities and challenges can be obtained by ASEAN. This means that ASCN cooperation must be well controlled because the city is a major player in the cooperation even though the agreement is at the national and regional levels.

Keywords: ASCN, digital, ASEAN, Collaboration, Innovation

I. Introduction

International relations in the digital era have undergone significant changes both from the substance of the issue and the increase in actors to the policy response to be able to adapt to these changes. The state as a rational actor must be able to innovate and adapt so that it collaborates with other actors to be able to meet their needs. This means that the State must be able to calculate all the possibilities and consequences of each policy response in the digital world. The digital age is inevitable by the State and the State is most responsible for safeguarding the sovereignty of the state and the sovereignty of its citizens from threats that can come from within as well as from outside. This threat can also be carried out by state actors and non-State actors.

Why this State is important in responding to this, Hamilton (1995) said that the development of international relations and diplomacy will always change based on four factors, namely a) changes in the international order, b) changes in the threat of the nature of war c) revolution of the role of the State and d) integration of Information Technology (Carlnaes, 2013). Therefore, these four points must be responded to creatively and innovatively by the State with a collaborative approach.

The author defines digitization citing the FDFA as writing that digitization is the technical process of changing the format of information from analog to digital format. This process results in structural changes in the form of new applications and systems to the economic, social, political, security, etc. fields. Digitalization is a new space just like land, sea, and air. A digital space is a space that provides the interaction of processes and not just devices but actors. The digital space provides a cross-border format (FDFA, 2020). Furthermore, in addition, the change in the direction of international relations in the digital arena: a) changes in the political, social, and economic environment in which diplomacy is carried out (e.g. the nature and distribution of power, new types of conflict, and the changing and interdependent nature of sovereignty in international relations); b) the emergence of new policy issues in foreign

[1] International Relations Department, University of Pembangunan Nasional "Veteran" Jawa Timur.

policy such as cybersecurity, data governance, e-commerce, and cybercrime, and; c) the use of digital tools in practice in international relations such as social media privacy, online conferencing, and big data analytics (Hone, 2021) (diplomacy.edu, 2021). Thus, these changes are both an opportunity and a challenge for the State in dealing with the threat of securitization in international relations.

Bjola and Holmes write that changes in the international system should make the State able to respond quickly because of the State. That this system change is called international management, meaning that in the digital era international relations practice must be able to innovate. Furthermore, that system changes in the digital era are called top-down structural exogenous shock. Exogenous means efforts to establish deep interactions through face to face. Still, the challenge is to build face-to-face communication in cyberspace. Furthermore, button up incremental endogenous shifting. Endogenous is defined by synthesis and analysis, technology, and big data. Thus, two things must be done, namely policy innovation and change adaptation (Holmes, 2015).

The international system is a structure composed of new hybrid C international relations actors, nonlinear, and only vaguely restricted. The new capabilities of the armed forces create new opportunities for the use of kinetic and non-kinetic forces in cyberspace (Neittaanmäki, 2011). Cyber security or Cyber security quickly evolved from a technical discipline to a strategic concept. Globalization and the Internet have given individuals, organizations, and countries tremendous new powers, based on ever-evolving network technologies. For everyone - students, soldiers, spies, propagandists, hackers, and terrorists - information gathering, communications, fundraising, and public relations have been digitized and revolutionized.

As a result, all political and military conflicts now have a cyber dimension, their size and impact are difficult to predict, and the battles that take place in cyberspace can be more important than events that occur on the ground. Like terrorism, hackers have found success in pure media hype. Like Weapons of Mass Destruction (WMD), it is difficult to retaliate against asymmetric attacks. The astonishing achievement of cyber espionage serves to demonstrate the high return on investment that can be found in computer hacking. The dynamic nature of the Internet offers benefits to attackers and defenders. Many cyber battles will be won by parties that use cutting-edge technology for greater gains. Although attackers have more targets to attack and More ways to attack them (Geers, 2011).

However, on the other hand, ASEAN countries form cooperation with cities to protect cyber security in each country. However, at the same time, these countries have the potential to create new threats by securitizing technology into digitalization. Currently, the agreement of ASEAN countries has reached the level of cities in each country. At the 32nd ASEAN Summit meeting, each ASEAN country agreed to form the ASEAN Smart City Network or (ASCN) cooperation.

ASCN is an innovation platform to create ASEAN as a smart city. ASCN is a form of ASEAN's commitment to creating connectivity between cities. As a result of the Report from ASCN 2022, there are 26 ASCN member cities. Some of these cities are Bandar Seri Begawan, Battambang, Phonom Penh, Siem Reap, Banyuwangi, Jakarta, Makassar, Luang Prabang, Vientiane, Johor Baru, Kota Kinabalu, Kuala Lumpur, Kuching, Nay Pyi Taw, Mandalay, Yangon, Cebu City, Davao City, Manila,

Singapore, Bangkok, Chonburi, Phuket, Da Nang, Ha Noi, Ho Chi Minh City (ASCN, 2022).

At the East Asia Summit on November 15, 2018, which was attended by ASEAN countries, and joined by several other countries such as Australia, China, India, Japan, the Republic of Korea, New Zealand, the Russian Federation, and the United States, ASCN's main objective is to improve the lives of ASEAN citizens, using technology and digital infrastructure to support the activities of ASEAN countries. By focusing on adopting an inclusive approach to smart city development that respects human rights and fundamental freedoms as set out in the ASEAN Charter. The Smart Cities Network in ASEAN also contributes to enhancing cross-cultural mutual understanding. ASCN cooperation uses an inclusive, transformative, innovative, and integrated approach. EAS fully supports cooperation to obtain economic, social, environmental, security, industrial, infrastructure, and health benefits. Previously, the commitment to the ASEAN Vientiane Smart City meeting was created in 2016 and adopted the ASEAN Connectivity Master Plan 2025, so all countries involved agreed to develop smart cities.

So that in the development of smart cities planned by ASEAN members, especially Indonesia, must prepare cyber security domestically and regionally in the face of cybercrime to protect people's networks and personal data. In addition, in building smart cities, they must also pay attention to various aspects that must be considered such as governance, human resource readiness, infrastructure readiness, finance, digital society, and sanctions that are prepared to reach the level of ASCN development idea. The author argues that the formation of ASCN is like a double-edged eye. It has a positive impact and has negative implications. For this reason, the author will describe and explain the prospects of ASCN digitalization as a threat as well as opportunities for cooperation at the city level.

II. Cybersecurity

Alford (2009) and Lee (2013) argue that cyber defense uses a variety of different sources and methodologies to mitigate active threats, using areas such as incident response, malware analysis, digital forensics, and event defense-driven intelligence. Cyber warfare is perhaps the biggest threat countries have ever faced. There has never been anyone who has the potential to affect the security of an entire country. And, never before has one person been able to cause the greatest possible damage in a cyber war. Cyber power will be revolutionary for warfare like air power, but the current domain vector will determine which country will hold cyber domination and what effect it will have (Neittaanmäki, 2011).

Cybersecurity and cyber resilience are the number one concerns for companies today. Organizations must protect their assets and defend themselves from threats and attacks to stay in business. A breach or breach can destroy a company's assets and/or reputation within minutes. Readiness is key, so if the unthinkable happens, your company will have the tools and action plan to counter and recover from the attack. Developing a cybersecurity and cyber resilience strategy that supports business and saves resources requires strategic planning. So, what must be accepted is that the war has not changed with the advent of cyber keywords. Cyber is just another way to conduct war, such as trench warfare, nuclear war, and other categories of wars established throughout history (Sweeney, 2020). Siber is the domain of war, This means that computer networks become seen as

spaces where we can maneuver, attack, and defend as we do in wars conducted in other domains (Oakley, 2017).

Then, cyber warfare, meaning cyber aggression between countries, is a phenomenon that is emerging increasingly important in international relations, with attacks on computer networks regulated by the state (or regulated by the state) that occurred in Estonia (2007), Georgia (2008), and Iran (2010). This method of warfare - given its potential to, for example, make planes fall from the sky or cause nuclear power plants to melt - can be as devastating as conventional means of conducting armed conflict.

Cyber from a technological point of view; the extent to which cyber attacks can be attributed to state actors; strategic value and the dangers posed by cyber conflicts; legal regulation of cyber attacks, both as a use of international force and as part of an ongoing armed conflict, and the ethical implications of cyber warfare. Thus cyber should be part of the State policy as a form of extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to the security of other states, or similar actions taken in response to serious threats to state security (actual or perceived) (Green, 2015).

III. Discussion

a. Digital Policy and Cooperation in ASEAN

Indonesia's policy regarding the implementation of smart cities has been going on for a long time. This is proven by the establishment of a Presidential Instruction in 2003 on governance based on e-government technology. The purpose of the instruction is to integrate accountable, flexible, and transparent governance. Effective, transparent, and accountable. E-Government is a form of technology-based management to its citizens by methods (G to C), (G to B), and relationships (G to G). The purpose of this service is to welcome the era of a Digitally Interconnected Community (DIC). The application of e-government as a means of creating good governance. Law No. 25 of 2009 concerning Public Services was issued to support the integration of governance based on Affirmation and Communication Technology (ICT), then issued No. 25 of 2009. From these rules, Indonesia adopted information technology integration in the public service governance system first.

Meanwhile, ASEAN, only started at the 28th ASEAN Summit on September 6, 2016, in Laos. Then on January 10, 2017, a Stand-Alone ACCC Meeting was held on the MPAC 2025 Implementation Arrangements. This collaboration contains points a) physical connectivity/infrastructure (physical), b) institutional, and c) inter-community (people to people). To implement MPAC, several mechanisms have been established to monitor and support its implementation. The mechanism in question includes the ASEAN Connectivity Coordinating Committee (ACCC) (ASEAN, 2017).

Cooperation in the field of digital innovation ASEAN has the potential to make a profit of US$ 625 billion by 2030 or around 8% of ASEAN's estimated GDP in 20230, which comes from increased efficiency, new products, and services, new digital services (such as data management and digital financial services); exchange of best practices for open data; and increased access to digital technology by Micro Enterprises, Small, and Medium Enterprises (MSMEs) (ASEAN, 2017).

In addition, the ASEAN ICT Masterplan (AIM) 2015 was ratified at the 10th ASEAN Telecommunication and IT Ministers Meeting (TELMIN) in January 2011. The document includes 6 strategic thrusts, namely: (i) economic transformation, (ii) community approach and empowerment, (iii) innovation, (iv) infrastructure development, (v) human resources improvement, and (vi) digital divide liaison (ASEAN, 2017). The implementation of AIM 2015 is coordinated by TELMIN by involving the ASEAN Telecom Communications and IT Senior Officials Meeting (TELSOM) and the ASEAN Telecommunication Regulators' Council (ATRC) in supporting policymaking. AIM 2020 prioritizes aspects of (i) ICT in the Single Market, (ii) New Media and Content, and (iii) Information Security and Assurance, without neglecting the 6 strategic thrusts listed in the document (ASEAN, 2017).

b. Securitization of Smart Cities Digitalization as Part of Cybersecurity Prospects

Cyber Age Command Control Theory According to USAF Col. John Boyd argues that in cyberspace what should be crippled is its physical and mental morals. In doing this, the actor can map the threat of uncertainty in cyber and direct the enemy to situations that are beyond its capacity. Furthermore, USAF (retired) Cyber Age Effect-Based Operations Theory Colonel John Warden argues that the most important thing is to paralyze the enemy's center of gravity through overall operation so that it quickly and precisely paralyzes the opponent (Neittaanmäki, 2011). This opinion shows that the securitization of cybersecurity is a concrete step by the state to prevent threats from the advancement of information technology and digitalization. This means that securitization is very important to show the quality, and capacity of the country in maintaining cyber resilience in the country.

Cybersecurity and cyber resilience, there are 6 steps to take. If done, an organization's cybersecurity and cybersecurity strategy will be comprehensive, functional, and durable, and receive ongoing support from cybersecurity governance management. The first step, initial planning, is the preparation of the second strategy development, strategy prospect management, third, cyber threat mapping, vulnerability, and intelligence analysis, fourth, risk calculation and cyber control, fifth, current threats and sixth target status assessment, Performance Measurement of Strategic Plan and Year-End Project (Sweeney, 2020). Although cybersecurity is securitized by the role of the state, the executors and impacts are local or local governments. Moreover, in a country in the form of unity and decentralization like Indonesia, of course, macro cooperation at the ASEAN regional level remains the executor area. This means that cyber resilience in the regions is very important to maintain cybersecurity stability.

The author has previously conveyed that this collaboration in digitalization has good prospects in the form of opportunities as well as challenges. Moreover, the cooperation carried out is on behalf of the region. The problem that exists is when the cooperation is carried out in multilateral meetings which are carried out only in the form of a Ministerial Conference or Ministerial Conference. This means that regional involvement is very small in obtaining knowledge socialization related to this digitalization cooperation. Meetings at the ASEAN regional level involve only Ministers, high-ranking officials, or relevant agencies. Meanwhile, the regions were not involved in the meeting as a form of contribution and participation. Kuznetsov said that the involvement of local governments or para-diplomacy in foreign policy should be synergistic. But it depends on the pattern

applied. Kuznetsov said that there is a formula used in the relationship between the center and the regions. However, what is relevant to the role of local governments in foreign policy, especially crucial issues, is the cooperative-coordinated and cooperative-joint formula. In addition, of the 12 elements of the para-diplomacy study dimension, cybersecurity is included in the dimensions of globalization and security/geopolitics. This means that globalization has implications for the country's activities in controlling its geopolitics, especially in the regions (Kuznetsov, 2015).

The involvement of local governments in ASEAN regional cooperation in the field of technological innovation and digitalization has been agreed upon in the establishment of ASCN. The goal is to create digital-based connections and cooperation for the ASEAN community and ASEAN countries. Smart cities as a form of ASEAN's commitment to follow up on several previously agreed meetings. Therefore, the existence of smart cities can create intense cooperation between ASEAN member states, especially implemented at the level of cities in ASEAN through ASCN.

There are five reasons why ASCN is important for ASEAN: a) to respond to urbanization and as a cultural heritage of ASEAN. At this point, ASCN will open opportunities for tourists to enter and travel in several cities in ASEAN more easily. With so many cultures available, it is enough to contribute 12 percent of ASEAN's GDP in the field of tourism; b) lifestyle health and welfare. At this point, it shows that the integration of technology in the health sector is a form of commitment to the SDGs, especially to protect the ASEAN community from extreme poverty which has been reduced from 138 million to 44 million people. The CLC survey shows that health and welfare issues are the main focus of ASCN; c) safety and security mean that this point shows that the progress of ASEAN's digital economy potential of up to $1 trillion is also threatened by cybersecurity. For this reason, the adoption of technological equipment, and the readiness of resources are needed to maintain cyber safety and security in ASEAN cities, c) environmental safety, at this point shows that the threat of disasters in ASEAN is quite large. ASEAN's losses reached 91 billion USD. The integration of technology in responding to disasters can minimize the casualties and implications of disasters such as early warning technology etc. d) Infrastructure development, this point shows that the construction of digital infrastructure development can increase the contribution of ASEAN opinions to 1.6 $ trillion. Then e) the progress of the digital industry and innovation, at this point ASEAN can be the key to global trade, especially in major cities in ASEAN.

There are about 144.800 pounds /100 or 100 people beating the United States and Europe which are only on 124 mobile phones/100 people. In addition, trade profits in ASEAN reach 5.3 $ USD annually. With the existence of digitalization and innovation, e-commerce opportunities in ASEAN are increasing (Hartati, 2022). That is why smart city cooperation is very important to create connections between cities.

Smart City has 6 indicators, namely Smart Governance (transparent, informative, and responsive government), Smart Economy (growing productivity with entrepreneurship and the spirit of innovation), Smart People (increasing Human Resources and decent living facilities), Smart Mobility (providing transportation and infrastructure systems) and Smart Environment (environmentally friendly natural resource management), and Smart Living (realizing a healthy and livable city) (Fathun L. M., 2018). From the meaning of smart cities, the 3 Indonesian cities involved in

ASCN do not include cyber security as part of the anticipation of ASCN digitalization. Based on data from shows that (ASCN, 2022) Banyuwangi City is the city that has the most projects, namely education, smart villages, tourism, stunting care, and plastic waste care. Then Jakarta only focuses on integrated transportation programs through JAKI, Jak Lingko, and health data (Corona). On the other hand, Makassar has projects in the field of smart care and tax services.

One example of Makassar Smart City Makassar consists of six modules. First, Smart Governance is optimizing public services by the city government. Second, smart branding is to increase awareness of the character of the city, especially for tourism. Third, Smart Economy is to build a good ecosystem and encourages a less-cash society. Fourth, Smart Living is how to create a comfortable life and increase awareness of health. Fifth, a Smart Society is to build an interactive and humanist society. Sixth, Smart Environment is to reduce and utilizes waste and creates a better source of energy. Makassar City was selected as one of the smart cities out of the government's 100 targets to create 100 smart cities in Indonesia in 2017 at the 2017 Smart City Award event which was handed over directly by Mengkominfo Rusdiantara. Moreover, Makassar City was selected for the Indonesia Smart Nation Award (ISNA) 2018 with the Most Perform in Smart City Initiative category in 2018 (Fathun L. M., 2018).

ASCN cooperation needs to get control from the central government. The securitization of smart cities is very important because the availability of resources in the regions is not good enough to counteract the potential for cybercrime in the regions. This means that there must be good training and debriefing so that smart cities do not become disasters in the regions. If you look at the data and representation of Indonesia's cybersecurity, according to the Director of e-Business of the Directorate General of Informatics Applications of the Ministry of Communication and Informatics Azhar Hasyim stated that Indonesia has the potential to become a major player in innovation and digital business. The strategy used is to increase start-ups. According to the Director of e-Business, to move towards the largest digital economy in Southeast Asia, several issues will be considered. Issues related to consumer protection, logistics problems of readiness, HR problems, and how the internet network can reach all regions and implement cyber security, one of which is with a partiality program or affirmative policy. Providing coverage to economically unfit areas with the Palapa Ring which will be supported by Broadband access. Also, the acceleration program later with data-driven satellites or High Throughput Satellite (Veren, 2016).

Regarding the needs of a smart city, according to the Director of e-Business, a cyber-based life with much greater challenges is needed. How is the implementation of IoT or the Internet of Things? Because this will enter all lines of life, as a reader of the situation, as a controller, and as a cyber-based mover going forward. The smart city once again returns to business processes, to problems that are then actualized into solutions by utilizing digital. IoT has a role in the future, but of course by creating these IoT-based solutions. One of the basic ways to overcome Smart City security gaps is a firewall, a network security system that monitors and controls outbound and inbound network traffic based on established security policies. Usually, firewalls provide a barrier between secure and trusted inner networks and external networks that are assumed to be unsafe, such as the Internet. But in certain cases, some systems are so

important that it is better not to connect to an outside internet connection at all.

Policies regarding data access control are also important steps to implement. In addition to guarding the system against cyberattacks, the human aspect of a system is also important. Establishing policies on who can access data, can provide strict access restrictions on data, and avoid unwanted access to important data (Veren, 2016). That is why smart cities promise great opportunities for collaboration but also promise potential cyber threats to private data.

The author interprets ASCN as governance of ASEAN's progress in making cities partners in foreign relations. But still, the city needs control and guard from the state to secure the data available in the city. Logically, cybersecurity in cities does not have implications for national security but will show national weaknesses. Because if cyber data is breached, it does not also dissolve the country or the city. But it only shows mental readiness and the quality of governance. Suddenly the government website is breached or in e-commerce, someone sends goods to a city government while the sender's data is unclear and the city government must pay the fee. And there are many other examples. Therefore, some of the arguments below as the main arguments in the prospects for cyber security in ASCN cooperation are:

1. The opportunity for ASCN to be processed (James, 2016):
    a. Realizing transparent, flexible, accountable city governance towards e-governance and good governance.
    b. Being able to show the competitiveness of the city based on integrated information technology connectivity will create security, comfort, and order in public services.
    c. The transformation of ASEAN society into a resilient digital society and towards good welfare.
    d. Make efficient use of physical infrastructure such as roads, environment, and economic instruments to create connectivity.
    e. Creating public participation in various state events both nationally and locally such as elections, regional elections, and other public participation that are integrated with information technology.
    f. Creating adaptation skills, and innovations in various crucial fields such as education, health, and social services. So, city life is needed to support the national interests of the country.

2. The challenges of ASCN
    a. Availability and Management of Information Data

    ASCN has the challenge of creating smart cities with urban governance to provide actual, factual, and accessible data in real-time. In addition, the data must be continuous and open to the public. So that the services and information provided to the public can be a reference for decision-making.

    b. Security Challenges in Smart Cities

    Smart Cities are usually handled by different institutions, without central management that can set standards for cyber security management throughout the organization. Another problem is the large number of devices connected to Smart City networks or systems, from water pumps to traffic lights, which were not originally designed to connect to the internet, so

they are not built with a cyber security approach (Kristo, 2015).

c. Smart City Development Investment is huge

The construction of smart city investment requires large funds. Therefore, the method of sharing management, sharing knowledge, and sharing donor investments will facilitate collaboration.
According to Setiawan, according to PwC's 2022 Digital Factory Transformation Survey, 64% of companies are still at the beginning of their digital transformation and only invest highly in high-income, a solid foundation driving scalable digitalization. Five factors must be prepared in digital transformation, namely a) organizational business strategy, b) increased internal resources, c) consumer experience design d) breaking through employee skepticism e) agile decision-making (Setiawan, 2023).

d. Information Technology Infrastructure

The construction of ICT infrastructure, from communication channels to sensors and actuators in physical space remains a major obstacle in taking the initiative of smart cities. Lack of infrastructure is a significant obstacle to achieving smart city goals. David Simon says that the world is heading towards digital democracy or internet democracy. Democracy is simply about the freedom to make responsible choices. He explained that information technology changes the format of political democracy and communication. This can be seen in the pattern when information is an important content in a democracy, the resulting impact is a) there is a gap between areas that have good internet access and infrastructure and minimal areas. The impact is clear on the regions will be minus information, b) the possibility of privacy violations because if it is connected to a connection, the world no longer has a private space, c) there is a change in the pattern of digitalization-based cooperation economy, the impact is that people are still dominant in the conventional economy whose basis is cash, and d) information technology makes the development of crime more flexible, more modern with all its models (Fathun L. M., 2018).

e. Social Adaptation

Social adaptation is like a system that requires social change from the habits of citizens in general and the people of the city in particular. If there is no control, it will create new social conflicts. Peter Harris and Ben Reilly (ed) are in a latent pattern of conflict where conditions have been broken where the forces that are part of the conflict become part of the complexity of the internal conflict. In a sense, the emphasis is conflict with positive and negative behavior. Positive in the sense that the structure is running and the negative is that it inflicts social-political losses. Therefore, it must be interpreted that what happens in the era of digital democracy is a method of meaning political conditions that are adversarial, (losing wins with risks), reflective (negotiation), or integrated (balancing of power) (Fathun L. M., 2018).

f. App development

Faster development of new and innovative applications will be necessary for citizens to take maximum advantage of the data being collected. If the development of the application is limited to the management of the city people will likely be disappointed with the slow development of the application. For example, one of the main reasons behind Android's success and the wide adaptation of its play store is a huge app base where countless apps are uploaded every day (James, 2016).

Furthermore, McQuail grouped the new media into four categories (McQuail, 2000). The first interpersonal communication media consists of telephone, handphone, and e-mail. Second, interactive playing media such as computers, video games, and games on the internet. Third, information search media in the form of search engines.

Fourth, the medium of collective participation such as the use of the internet to share and exchange information, opinions, and experiences through computers where its use is not only for tools but also creates affection and emotion. It is undeniable that the presence of new media in society itself creates a new order of society, namely the birth of the concept of an information society. As McQuail points out that society will then depend on electronic information and complex communication networks and allocate most of its resources to communication activities (McQuail, 2000).

Furthermore, Kaplan divides six types of social media, collaboration projects (e.g., Wikipedia), blogs and microblogs (e.g., Twitter), content communities (e.g., Youtube, social networking sites (e.g., Facebook), virtual games (e.g., World of Warcraft), and virtual social (e.g., second life). Social networks are central to the birth of virtual society. Everyone in cyberspace can connect with their community to communicate. Some of the big social events include Facebook, Twitter, Instagram, Path, and Snapchat (Kaplan, 2010).

The presence of social media in politics does not only add to the positive impact where in the era of digital democracy social media is often used to provide knowledge related to certain candidates. Social media in the era of new media is a concrete instrument for conveying messages to unreachable constituents. This means that the new media has a different where without having to meet face to face but every biased idea is obtained through the media. Collaboration between politics in the digital era and social media is also an instrument of the increasing maturity of a country in making democracy a political system of government. Social media is an inseparable instrument in the era of digital democracy. This means that social media complements the model of political communication carried out by candidates through the classic verbal way of political rhetoric. Social media provides a democratic space to advise, provide arguments and critique the political system of government.

IV. Conclusion

The author argues that ASCN cooperation is an advancement in public service governance in the ASEAN region. ASCN governance will create connections between cities and government making it easier to collaborate. ASCN is an innovation to answer the challenges of advances in information technology in public service governance. But it

should be noted that progress always goes hand in hand with challenges. Therefore, because of the ASCN, agreements at the regional level carried out by Ministry and high-ranking officials must involve the local government. Because although the cooperation is at the level of high-ranking officials, the execution is at the local level.

ASCN's cooperation through smart cities is a commitment to creating a digital society and digital connections in every area of life in the ASEAN region. It is hoped that through the cooperation of ASCN, it will create good benefits for the government and society and the progress of ASEAN innovation. However, it must be noted that such progress is a potential opportunity and a challenge. So, collaboration, coordination and sharing, and socialization are needed in policy making. It takes good knowledge to manage so that it does not become a target for hackers to carry out data security cybercrimes in the area. Especially Indonesia, which is still relatively weak in data protection and privacy on the internet. Though ASEAN is the most mobile phone user in the world. With this collaboration, it is hoped that it will be able to increase synergy and collaboration at the local, national, and regional levels.

Works Cited

ASCN. (2022). *ASCN Monitoring and Evaluation Report 2022 (As of 21 September 2022).* Jakarta: ASCN.

ASEAN. (2017). *ASEAN Selayang Pandang.* Jakarta: ASEAN.

Bryman, A. (2012). *Social Research Methods 4th Edition.* Oxford: Oxford University Press.

Buzan, B., Weafer, O., & Wilde, J. d. (1998). *Security A New Framework For Analysis.* London: Lynne Rienner Publisher Inc.

Carlnaes, W. (2013). *Handbook Hubungan Internasional.* Bandung: Nusamedia.

Fathun, L. M. (2018). Membangun Indonesia "Resolusi Konflik Sosial Lintas Perspektif". In *Membangun Indonesia "Resolusi Konflik Sosial Lintas Perspektif".* Jakarta: IQRA.

Fathun, L. M. (2018). Pariwisata Era Ekonomi Digital: Sebuah Implementasi Pilar Kebijakan Poros Maritim di Era Jokowi dalam Konteks Paradiplomacy. *DEP (Jurnal Dinamika Ekonomi Pembangunan)*, 49.

FDFA, S. F. (2020). *Digital Strategy Foreign Policy 2021-214.* Swiss: Swiss Federal Departement of Foreign Affair FDFA.

Geers, K. (2011). *Strategic Cyber Security2011 NATO Cooperative Cyber Defence Centre of Excellence.* New York: CCD COE Publication .

Green, (. E. (2015). *Cyber Warfare A multidisciplinary analysis .* New York: Routledge .

Hansen, B. B. (2009). *Evolution of International Security Studies.* London: Cambridge University Press.

Hartati, I. d. (2022). Pengembangan Kerjasama ASEAN Melalui ASEAN Smart Cities Network (ASCN). *SPEKTRUM*, Vol 19, No 1,38.

Holmes, C. B. (2015). *Digital Diplomacy Theory and Practice.* New York: Routledge.

Hone, J. K. (2021). *2021 The Emergence DigitalForeign Policy.* Mlta: Diplo Foundation Anutruf .

Iavor Rangelov, M. K. (2014.). *The Handbook of Global Security Policy. .* London: WILEY Blackwell.

James, C. (2016, November). *ACS.* From ACS: Cyber Security, Threats, Challenges, Opportunities. https://www.acs.org.au/content/dam/acs/acspublications/ACS_Cybersecurity_Guide.pdf

Kaplan, A. M. (2010). *Users of the World, Unite! The Challengers and Opportunities of Social Media. .* Business Horizons.

Kristo, Y. (2015). . *Mengatasi Tantangan Implementasi Smart City. DetikNet [Online] http://inet.detik.com/read/2015/1*

2/06/101802/3088965/398/mengatasi-tantangan-implementasismart-city.

Kuznetsov, A. S. (2015). *Theory and Practice of Paradiplomacy: Subnational Governments in International Affairs.* New York: Routledge New Diplomacy Studies.

McQuail, D. L. (2000). *Communication Theory (4th edition).* London: Sage Publications.

Neittaanmäki, (. E. (2011). *Cyber Security: Power and Technology.* New York: Springer.

Neuman, W. L. (2014). *Social Research Methods:Qualitative and Quantitative Approaches Seventh Edition.* England: Pearson Education Limited.

Oakley, J. G. (2017). *Waging Cyber War Technical Challenges and Operational Constraints.* New York: Owens Cross Roads, AL.

Setiawan, A. (2023, February 23). *Digitally Transform or Perish: The Future of Economy is Digital and Inevitably Your Business Must Adapt | Multimatics* . From https://diginovation.multimatics.co.id/digitally-transform-or-perish.aspx: https://diginovation.multimatics.co.id/digitally-transform-or-perish.aspx

Sorenson, G., & Jackson, R. (2014). *Pengantar Studi Ilmu Hubungan Internasional.* Yogyakarta: Pustaka Pelajar.

Sweeney, C. A. (2020). *Cyber Strategy Risk-Driven Security and Resiliency.* New York: CRC Press Taylor & Francis Group .

Veren, N. (2016, June 20). *KOMINFO RI*. From KOMINFO RI: MENKOMINFO " badan cyber nasional demi indonesia digital" https://kominfo.go.id/content/detail/7693/badan-cyber-nasional-demi-indonesia-digital/0/sorotan_media

Woodside, A. (2010). *Case Study Research : Theory,Methods and Pratctice* . Boston: Emerald Group Publishing Limited .

Yani, A. A. (2005). *Pengantar Studi Ilmu Hubungan Internasional.* Bandung: Rosdakarya.