International Conference on Business Economics, Social Sciences & Humanities

The Internet of Things (IoT) Impact on Global Security

D Triwahyuni
Program Studi Ilmu Hubungan Internasional, Universitas Komputer Indonesia

Email : dewi.triwahyuni@email.unikom.ac.id

Abstract. The purpose of this study is analyze from the perspectives political science and international relations the role of this emerging technology in global affairs, especially on the potential strategic impact of the IoT impact on Global Security. The Internet of Things (IoT) will impact every area of Global Affairs from security to business to international development and aid. As objects, data, systems and people become part of this global interconnected network, business models, stakeholder interaction, systems of governance and security threats will irrevocably change. Governments, not-for-profit organizations and business will have no choice but to innovate, optimize and incorporate an increasingly disparate array of digital touchpoints when engaging with stakeholders, assessing threats and collaborating with partners. This is not a technological problem; it is a strategic issue that has no tool or program that will solve the problems that this technology will bring. To answer the problem of research, researcher use qualitative research design. Researchers use primary sources in the form of official state documents and secondary sources in the form of interviews with experts, through journals, dissertations and related research. The results of the study found that the massive development of IoT creates information vulnerability that threatens national security as well as global security.

1. Introduction

In the era of digitalization, there was an increase in connectivity between devices, citizens and governments which changed many aspects of people's lives. The Internet of Things (IoT) enables physical objects to see, hear, think and do work by making them communicate together, to share information and coordinate decisions. IoT will drive the development of a number of applications that take advantage of the potentially large amount and variety of data generated by these objects to provide new services to citizens, companies and public administrations [1].

Since it was first introduced in 1999, IoT was created to connect everything with anyone, anywhere and anytime so that it creates interactions between the physical and virtual worlds [2]. Vermesan define Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things or objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things or objects to create new applications/services and reach common goals [3]. Berte quotes from Oxford Dictionary defines IoT as: A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data [4].

According to the Cisco Internet Business Solutions Group (IBSG), the IoT is simply a time when more "things or objects" are connected to the Internet than people. It is at this point that IoT changes the way humans interact and ultimately has an impact on the concept of security [5]. Technological improvement which finally created IoT is continuous and ubiquitous. It impacts our lives because each new advance alters how we communicate and analyse information; it changes how we interact with the world. Change can lead to dependence, and therefore cyber con ict and cyber war have become dominating issues of concern in the realm of international relations. From the telegraph to the telephone, we become dependent on each technological advance, and this dependency creates a perception of vulnerability [6].

ISBN: 978-623-95562-0-4

The purpose of this research is to find the impact of the IoT on global security according to political science and international relations perspective. Therefore, researchers chose to use qualitative methods to analyze this global phenomenon by looking for variables that can explain changes in global security with the development of IoT.

2. Method

This research uses a qualitative method by describing the facts about the development of Internet of Things (IoT) related to interactions between international relations actors. The description of the research object is then analyzed to find out its impact on global security. The research method uses data collected from international journals using a search engine on the internet and searching for sources from books or official documents. This study also obtained a number of data from KOICA Cyber Security Center-ITB Bandung and Indonesian Institute of Science (LIPI). Some other data obtained by interviewing global security expert, namely Arry Bainus from Universitas Padjadjaran.

3. Results and Discussion

3.1. How Internet of Things (IoT) Change Everything

The concept of the internet of things includes 3 main elements, namely: physical or real objects that have been integrated into sensor modules, internet connections, and data centers on servers to store data or information from applications. The use of objects connected to the internet will collect data which is then collected into"big data" is then processed, analyzed by government agencies, related companies, and other agencies and then used for their respective interests.

The rapid development of the Internet of Things (IoT) also encourages various sectors of life in the world community. Among them is the exponential growth rate in electronic components trading. According to the latest data released by UNCTAD, the demand for electronic components used in IoT devices increased the international import trade value for information and communication technology (ICT) equipment to reach $ 2.1 trillion in 2017. This is the first time the value of global imports of ICT goods has soared. since 2014. This represents an annual growth rate of 6%.

The Commission of the European Communities sees IoT as a form of technology / internet development which was originally limited to connecting networks with computers but now has a wider scope, namely connecting networks with other physical objects or interconnected objects [7]. Meanwhile Patel [8] categorizes IoT into three interaction relationships using the internet, namely between: (1) people to people (2) people to machine / things (3) things / machine to things / machine. From some of these explanations, IoT is a big network where everything is connected (people-people, people-things, things-things) using the internet.

Today, the IoT consists of a collection of distinct and custom made networks. Today's cars, for example, have multiple networks to control engine functions, safety features, communication systems, and so on. Commercial and residential buildings also have various control systems for heating, ventilation and air conditioning (HVAC); telephone service; security; and lighting. As IoT evolves, these networks, and many others, will be connected with additional security, analytics, and management capabilities (see Figure 1). This will allow the IoT to become stronger in the ways that it can help people achieve their goals [5].

ISBN: 978-623-95562-0-4

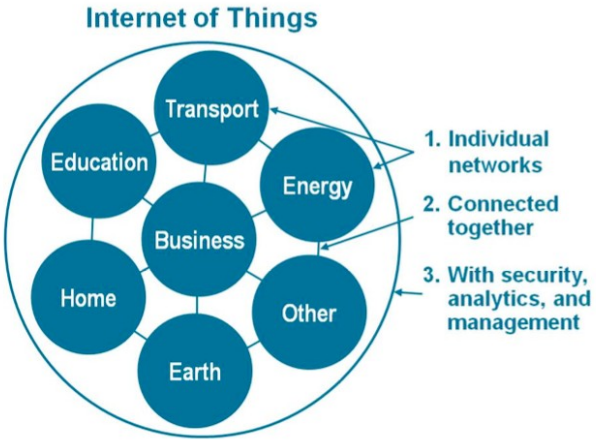

Figure 1. IoT can be Viewed as a Network of Networks
Source: Cisco, IBSG, April 2001

The level of human dependence occurs because the applications of IoT are numerous and varied, permeating almost all areas of the daily life of individuals, companies, and society and the world as a whole. IoT applications include "smart" environments / spaces in domains such as: Transportation, Buildings, Cities, Lifestyle, Retail, Agriculture, Factories, Supply Chains, Emergencies, Health Care, User Interaction, Culture and tourism, Environment and Energy [8]. Below are some of the IoT applications (**see** Figure 2).

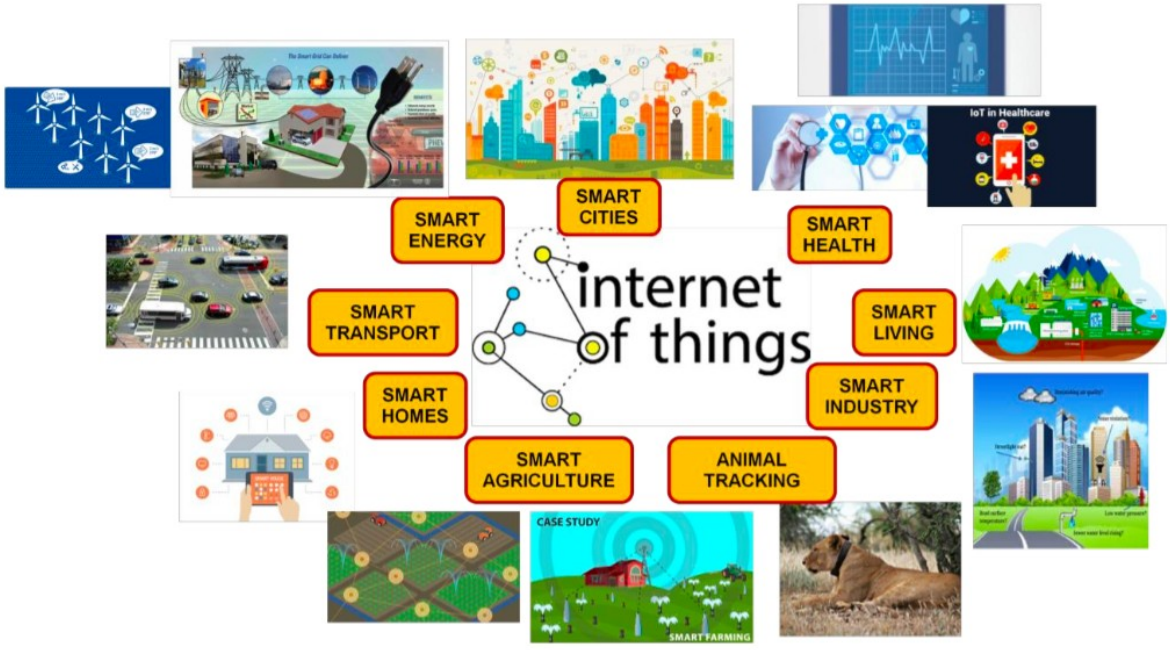

Figure 2. IoT Applications
Source: Patel & Patel (2016)

Along with the rapid penetration of global networks and the advancement of the mobile internet, an organization's information security vulnerabilities from cyber threats are increasing. IoT has spawned a number of crimes using information technology such as carding crimes (credit card fraud), ATM/ EDC skimming (early 2010), hacking, cracking, phishing (internet banking

ISBN: 978-623-95562-0-4

fraud), malware (viruses / worms / trojans / bots). The rise of these threats is an impetus for broader cooperation in cybersecurity with countries around the world [9].

3.2. IoT and Global Security Vulnerabilities

The application of the IoT network is a complex process. The main problem that is often taken into consideration is the safety factor. Based on well-known security service providers such as Gartner, Cisco and Symantec, the definition of network security means protection of the network and data from unauthorized access to mitigate disruption in the business processes of a business group or the administration of government activities. The risks faced in dealing with cyber-attacks also cover several aspects. In general, this form of attack has 3 main objectives, namely (1) to disrupt business processes; (2) information leakage; and (3) taking over a system.

The conclusion is that the development of the Internet of things has been going on for about 3 decades, and at this time almost all the equipment we use in our daily lives can be controlled and monitored using the IOT, where the majority of the process is carried out with the help of sensors on the IOT. This sensor functions to convert raw physical data into digital signals and send it to the control center. In this way, we can monitor environmental changes remotely from any part of the world via the internet.

The threats that can affect IoT entities vary widely, depending on the target of the attack. Roman in categorizing threats to IoT as follows [10]:

1. Denial of Service, an attack that causes parties the valid one cannot access the service.
2. Physical damage to objects in IoT.
3. Eavesdropping; passive attack that can be done on various communication channels with a purpose extract data from the information stream.
4. Node capture; the attacker extracts information from node or from other infrastructure that has data storage capabilities.
5. Controlling; where the attacker was trying to get to control of IoT entities and disrupt services and data from these entities.

Various types of threats above, can attack various entities in IoT, especially RFID and sensor networks.

From the description of security issues above, we can see a variety of security and privacy issues in IoT that can threaten IoT entities and can harm and endanger users. For example, theft of sensitive information such as bank account passwords, easy access to personal data by unauthorized people which can be a way to break into personal and institutional finances. In addition, because of its interconnectivity nature, an attack on one piece of equipment will affect the integrity of the other connected equipment. Security and privacy issues that could threaten the integrity and confidentiality of data and could also harm users were discussed. These security issues can hinder the development and implementation of IoT in various fields. So it can be concluded that there is still much that needs to be done to make IoT a part of everyday life.

Kaspersky Lab's research results One of the most popular attacks and infection vectors against devices remains cracking Telnet passwords. In 2018 the country that experienced the most frequent attacks was Brazil (23%). The second position is occupied by China (17%). Russia occupies the 4th position (7%). Overall for the period January 1 - July 2018, our Telnet honeypot recorded more than 12 million attacks from 86,560 unique IP addresses, and malware was downloaded from 27,693 unique IP addresses [11]. The top 10 countries most frequent attacks can see in Figure 3 below:

ISBN: 978-623-95562-0-4

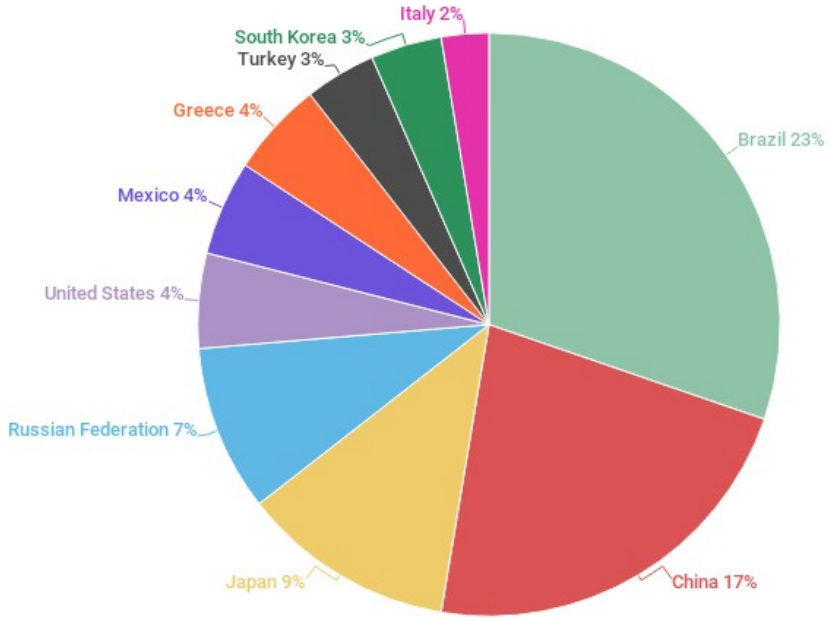

Figure 3. The Top 10 countries from which our traps were hit by Telnet password attacks
Figure was adopted from https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

There are two types of cyber threats to infrastructure. First, threats to communication and information infrastructure. Second, threats to all other forms of infrastructure that depend on strong communication systems. In the absence of agreed policy-related activities and technology at the interface between information systems and infrastructure systems, it is easy to imagine the potential for damage [12].

4. Conclusion

The results of the research conclude that IoT has developed rapidly over the past 3 decades and changes the interaction patterns that occur in everyday human life. Where the Internet that can be used on all devices allows users to interact directly with the machine. Because, this is in line with the purpose of IoT by connecting almost all devices to interact every day with humans via an internet connection. IoT devices may leave you vulnerable to hacks and security issues. Ultimately, the viewpoint of global security threats extends from physical threats to virtual threats. The wider the IoT implementation, the greater the global security fragility.

References

[1] Wilianto, W., & Kurniawan, A. (2018). Sejarah, cara kerja dan manfaat internet of things. *Matrix: Jurnal Manajemen Teknologi dan Informatika*, *8*(2), 36-41.

[2] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137.

[3] Vermesan, O., & Friess, P. (Eds.). (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.

[4] Berte, D. R. (2018, May). Defining the iot. In *Proceedings of the International Conference on Business Excellence* (Vol. 12, No. 1, pp. 118-128). Sciendo.

ISBN: 978-623-95562-0-4

[5] Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, *1*(2011), 1-11.
[6] Valeriano, B., & Maness, R. C. (2018). International relations theory and cyber security. *The Oxford Handbook of International Political Theory*, 259.
[7] Comission of The European Communities. (2009). *Internet of Things-An Action Plan for Europe*. Brussels.
[8] Patel, K. K., & Patel, S. M. (2016). Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International journal of engineering science and computing*, *6*(5).
[9] Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi*, *8*(2), 137-144.
[10] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266-2279.
[11] Kuzin, M., Shmelev, Y., & Kuskov, V. (2018). New trends in the world of IoT threats. *Kaspersky Lab*.
[12] Chourcri, Nazli. (2012). Cyberpolitics in International Relations. London. The MIT Press.

ISBN: 978-623-95562-0-4