Anticipating Cyber Security Challenge In The Era of Internet of Things (IOT) : Internet Eavesdropping

Rudy Agus Gemilang Gultom
Indonesia Defense University, Bogor, Indonesia

Abstract

Nowadays, in the era of Internet of Things (IoT), the activity of information tapping over the Internet is one of the negative impacts of the interconnectivity between the Internet users and the ease of the process of exchanging data on the Internet. The disclosure of classified sensitive or confidential information or the loss of important documents is the result of information that is not well protected. Consequently, Internet users need to know more information about eavesdropping via the Internet in order to anticipate cyber security challenge.

KEYWORDS–Internet; Internet of Things (IoT); information, eavesdropping; cyber security.

1. INTRODUCTION

In the era of Internet of Things (IoT), many countries in the world are heavily use of Internet.On the other side, because of the adverse use of the Internet various resources on Internet can be utilized harm critical infrastructures or sensitive information systems that can threaten national interests. Internet dependency or cyberspace. Hiding terminology is an electronic attack, where digital communications are interrupted by an individual who is not intended to. It is done in two main ways: directly listening to data loss or weakening of digital or analogue voice communication or any form of communication (Technopedia, 2019).According to Indonesian dictionary, wiretapping terminology is the process, form, gravitational act, means to listen (to record) without the knowledge of any person (confidential talk)for example, the phone sounds (or phone numbers) are a third party telephone and internet call monitoring that is monitored in secretly. User'sphone communications may be monitored or recorded illegally by third party. Internet broadcasts on Information and Communication Technology (ICT) progress are largely organized by state actors or non-state actors that can become a serious cyber attack. Cyber attacks on the Internet are different, ie hacking, phishing, IP spoofing, listening / wiretapping, etc., inspired many countries and then created their national Cyber Agency to protect their national interests from cyber threats or cyber attacks. For example, US Cybercom, Chinese PLA's Blue Army, Korean's KISA or Israeli'sIDF 8200. Moreover, through National Institute of Standards and Technology (NIST), Cybersecurity has decided to protect or defend cybercrime from the cyberspace. The Indonesia Government,in may 2017, established of the National Cybercrime and Coding Agency (BSSN), 2017 May 23. According to Hootsuite statistics, 2019 Indonesia ranked 5th in the world in January after the world's largest Internet users, China, India, US, and Brazil. As a matter of fact, the Internet users population in Indonesia has reached 150 million users. (see Fig. 1).

Figure 1. Internet users in Indonesia (in January 2019)

2. UNDERSTANDING THE GLOBAL DOMAIN CHALLENGES

Nowadays, in order to understand the challenges of cyber security in cyberspace, it requires understanding of the cyber issues. A nation should aware to fully imagine cyberspace is international boundary space, the universe is smaller and indefinitely, which brings new challenges to the IoT era. The incompatible international understanding of the Cyber space and how the government deals with serious problems, especially if onenation tries to claim that the global domain (cybercrime) is part of the sovereignty of a country in unilaterally way.This contradicts with the requirements of those countries that adopt international treaties like the UNCLOS 1982. It has been clearly defined in UCLOS 1982 that state or nation has responsibility of a sovereign state in the use and management of the world's oceans or EEZ (Exclusive Economic Zone) and its natural and environmental resource management. In fact, cyberspace is viewed as non-physical, frontier, stateless, and endless for all.The US Government through the US DoD has declared Cyber Security as a global domain in information encompassing as a network of information technology infrastructure and residency information, as well as Internet telecommunication networks and computer network systems. The US DoD declares a definitive termsfor cyber security as "the use of cyberspace capabilities where the primary goal is to achieve goals or via cybercrime (US DoD, 2011)."

Indonesia, will also facing global cybersecurity challenges as well as the same use of cybercrime (internet). This challenge can have an impact on cyber threats, such as cybercrime, cyber radicalism, cyber-terrorism, etc. for Indonesian state security. The infinite, incomprehensible and indefinite peculiarities and attributes of the Cyberspace make cybercrime as a transnational crime. This condition makes global role of cyberspace is a national priority that should be comprehensive, complete and effective. Comprehensive understanding of the global domains of cybersecurity (Internet) in the international community plays an important role in preventing predictability of complex and dynamic cyber security challenges in the international community, so the country can protect its integrity and sovereignty from cyber threats or cyberattacks, that is, Internet telephony or wiretapping - cybercrime through legal framework development.

3. INTERNET EAVESDROPPING CASES

In terms of eavesdropping or wiretapping issues, there are many incidents in the world (including Indonesia):

- In 2007-2009, BBC said that according to Lieutenant General Marciano Norman, the chief of BIN (Indonesia intelligence agency),Australian intelligence agency, has tapped phone communication with several Indonesian leaders (BBC, 2013).

- In 2013, NSA outbreak news by former intelligence analyst Edward Snowden, such as:
  a. Australian intelligenceagency wiretapping phone calls President of Indonesia Mr. SBY and Mrs. Ani Yudhoyono (Kompas, 2013).
  b. Wiretapping German Chancellor, Angela Merkel phone calls.
  c. Wiretapping French President, Francois Hollande phone calls.
  d. Wiretapping Mexican government, phone calls.
  e. WiretappinhgBrazilian President Dilma Rousseff phone calls.

- In Panama, April 2016In Panama (April 2016), There were "leakaged" through Internet about 11.5 million classified documents in 2.6 Tera Bytes, consist of higly classified data from 214,000 institutions in the world which is hosted and leaked from Panama's famous service company, Mossack Fonseca. Those confidential files are leaked, such as, 4,804,618 email files, 3,047,306 database files, 2,154,264 PDF files, 1,117,026 images files, 320,166 text files and 2,242 other format files. A suspicious "leakage" of 11.5 million sensitive files is made by hackers or by the people from internal of "Mossack Fonseca" company it self (see Fig. 4).

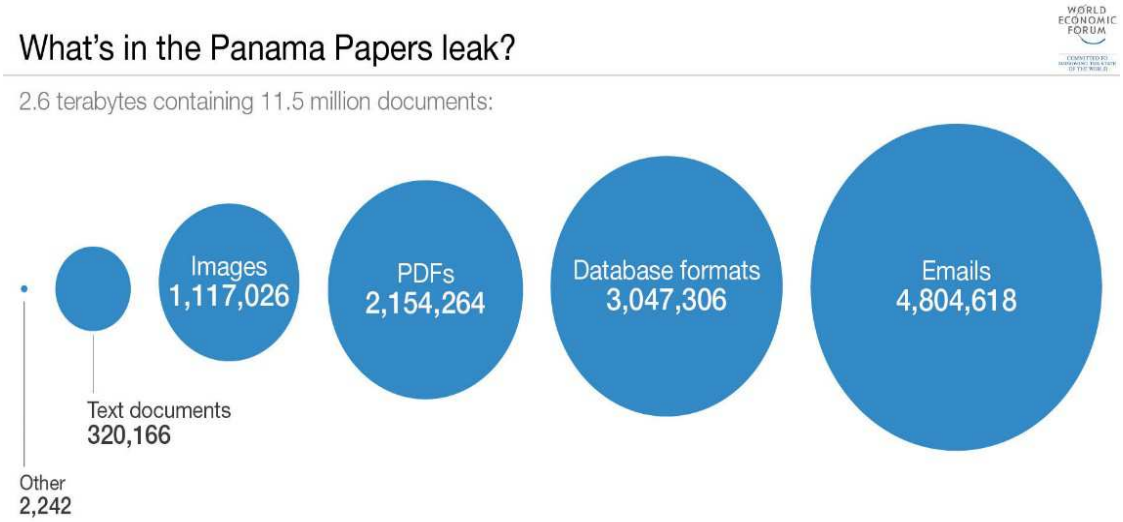

Figure 2. The Scale of Panama Papers Leak

- In USA, October 2016, the US government "blamed" the attacks on political hackers and wiretaps on the part of Russia's US President. According to CIA agency intelligence, Russian hackers have successfully succeeded in wiretapping information and information systems directly linked to the US electronic voting system, although this "accused" was rejected by the Russian

government. An important lesson that you can learn from this phone number is the need to pay attention and protection in a cybersecurity environment by choosing a presidential election or a regional leader by choosing an email system where the role of the encryption system is critical to avoiding the phone call or the internet.

4. METHODS

In this article, authors focus on research that contributes to the phenomenon of wiretapping over the internet using the various data sources on Internet (Baxter and Jack, 2008). The use of real-time analysis to explore the depth of the different aspects of "real-life" issues of eavesdropping phenomenon that can jeopardize the important national infrastructure and sensitive information communications systems to ensure that phenomena are investigated and detected with a few lens oscillations. This research has been done by method of qualitative, where data is taken from case study, which is related to the audition or phone call. The data obtained in the research design is quantitatively analysed and described on the basis of the researcher's thoughts. Comparative studies are performed by comparing cyber security issues that happens in many countries, wheredata required was collected via internet literature survey for recent 5 years (see Fig. 3).

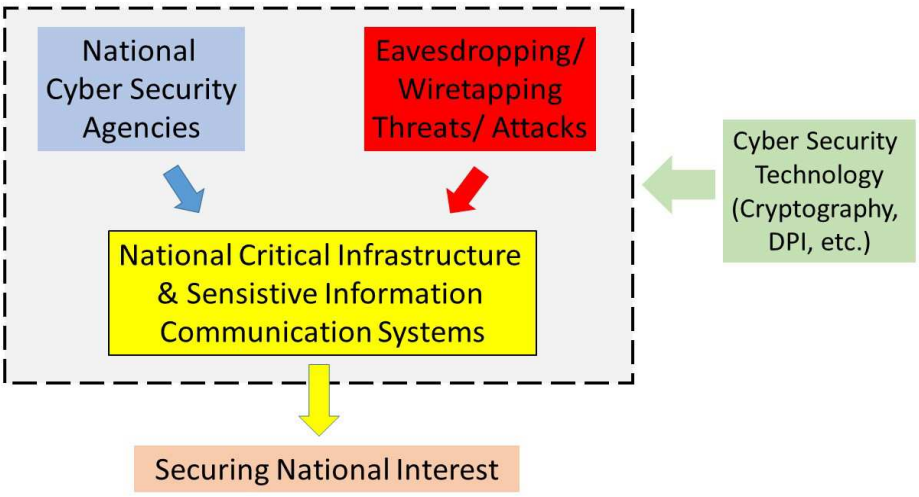

Figure 3. The Research Design Framework

5. RESULT

Based on conventional telephone technology technique, authors try to concentrate on the eavesdropping or wiretapping through the Internet. The internet eavesdropping perspective terminology is now being considered by the BKD DPR RI (the office of the Indonesia House of Representatives) who prepared the wiretapping over Internet law. Because Internet eavesdropping is one of the clever fraudulent methods of the Internet access, which uses special obstacle tools and can only be done by "certain users or parties" that have special abilities or capabilities. Internet eavesdroping activities are the same as theft data / information or trafficking victim network, which has become a direct target on the internet.

As it can be concerned, the term "Internet eavesdroping" might be compared with "listening" on the Internet terminology. For Internet utilizations, users should consider fully understanding of the Internet network systems works and also various hacking utilities can be used by hackers. As it is known, Edward Snowden, formerly a

National Security Agency analyst, that has uncovered sensitive NSA documents where the US government can control the digital activities of all Internet citizens in the world (Paramadina, 2015)

To answer question regarding how the internet eavesdropping works. Basically, the third party or the hacker “hear” or monitor the transmission of data or information transmitted through the LAN (Local Area Network) network between the targeted users. When Internet users are communicating via a network, they send data transmission signal between internet users. The transmission of data signals use TCP/IP data communication protocol or Internet Protocol, based on7th layers of Open Source Interconnection (OSI layers) data flow mechanism (see Fig. 4).

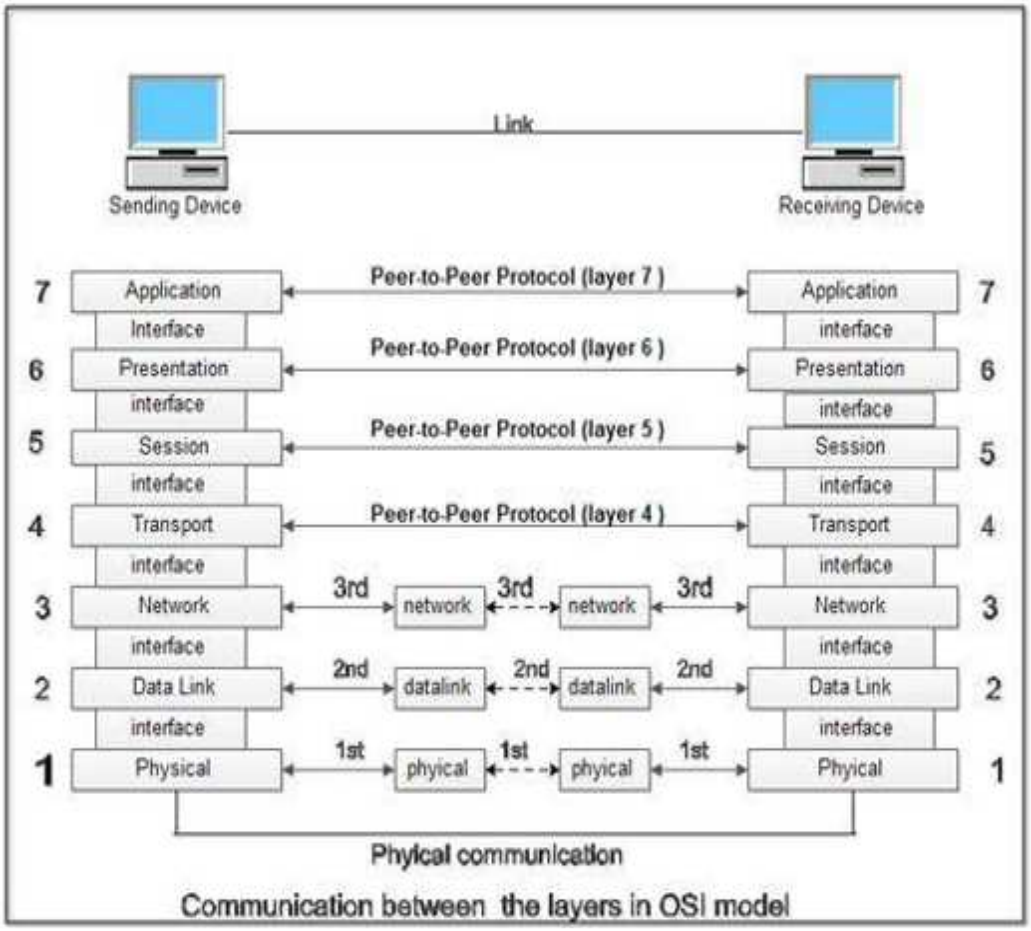

Figure 4. Data Communication through 7 Layers of OSI model

As it can be seen, from figure 4, data signal or information transmitted from sending device (PC, Laptop, etc) to the receiving device (PC, Laptop, etc) over the TCP/IP network. The data signal or information sent through Internet by following the 7 layers of OSI data flow mechanisms where the data signal or information can be easily "read" by third party users or hackers.

Therefore to protect data signal or information we need data or information security mechanisms, i.e., encryption technique, etc. One of famous technique is Deep Packet Inspection (DPI), this technique is used as an advanced methods to monitor as well to protect data signal and sensitive information sent over the Internet. DPI is simply a tool for internet / packet data monitoring (see Fig 5).

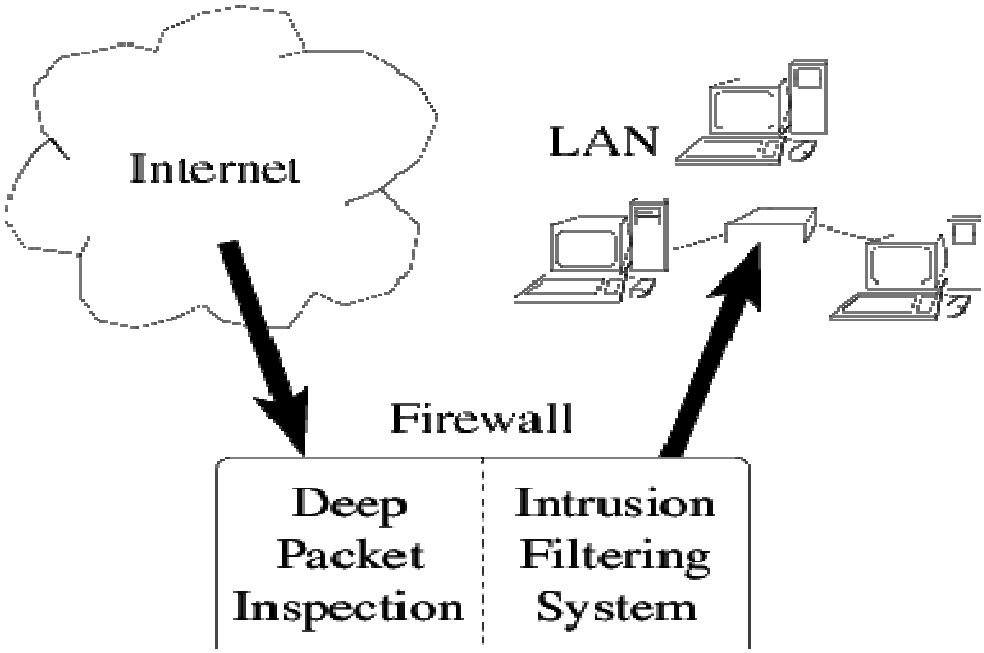

Figure 5. Deep Packet Inspection (DPI) combined with Firewall

The DPI provide depth analysis of data signal or information transmissions. DPI works properly by supporting parameters, i.e., the origin sending and revceiving device information, types of data, content of data, and contain of keywords in the data signal transmission. These settings will be useful when there are too many data passing through the network. Knowing inaccurate data parameters might be accepted where specific data or information might be presented and analyzed. DPI inspects the upper stream (data origin) and the bottom (location data) and focus on minimizing the data that have been missed. DPI is implemented to achieve service quality improvement, Internet usersprotection from harmful contents, such as virus, hoax, etc. As we may know, Internet transmissions occurs in countries over the world. Some countries implement the law that statesis strictly prohibitedto wiretapp the secrecy of their citizens. Meanwhile, some countries allow the state to wiretapping their citizens in terms of nastional security matters.

The DPI can be used also to monitor the mobile networks. As the development of mobile networks utilizations in the world, the traffic volumes in mobile networks are rising and end-user needs are rapidly changing constantly (see Fig. 6). As known, Mobile network operators need more flexibility, lower network operating costs, faster service roll-out cycles and new revenue sources. 5G and future networks aim to deliver ultra-fast and ultra-reliable network access capable of supporting the anticipated surge in data traffic and connected nodes in years to come. Several technologies have been developed to meet these emergent demands of future mobile networks, among these are Software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing. The security challenges these new technologies are prone to in the context of the new telecommunication paradigm. There are multi-tier component based architecture to address these security challenges in the market, for example the Software Defined Mobile Network (SDMN), proposed by Madhusanka LiyanageIjaz et all (2017), wheretheir DPI proposal are designed to handling security at different levels to protect the network and its users also appropriate methods for elevated security in the control and the data planes of the networks.

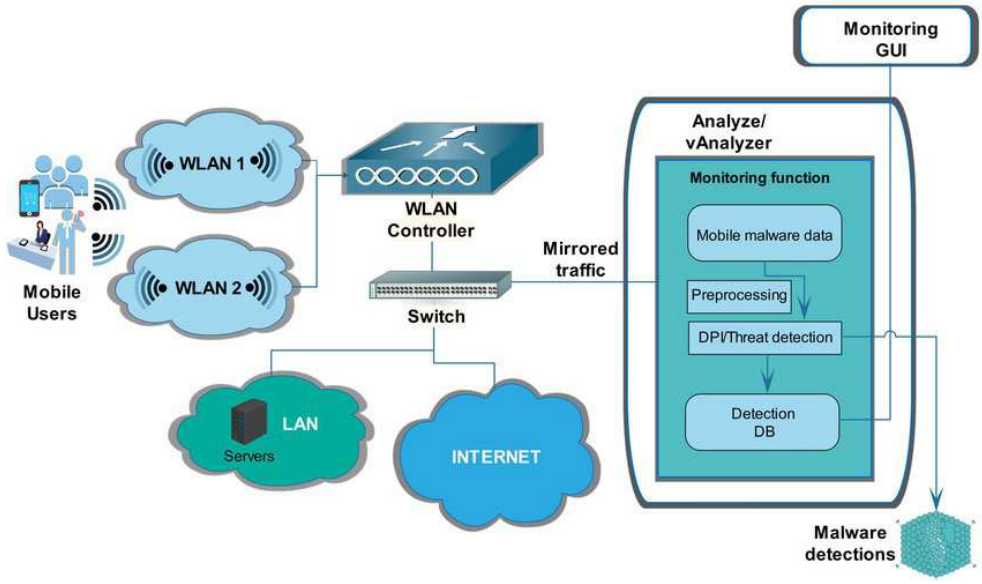

Figure 6. Deep Packet Inspection (DPI) combined with Firewall

Another example of DPI utilization is in China, the internet userscan not accessing foreign portals or websites, such as google, facebook, youtube and many others (see Fig. 7), where Chinese government has regulation to regulate incoming or outgoing data signal or information into its internet territory using Greatwall of China DPI mechanism. To monitor China's entire data traffic, DPI will be executed or checked to filter all web sites from outside China. China has also placed a special keyword filter to protect their national interests.

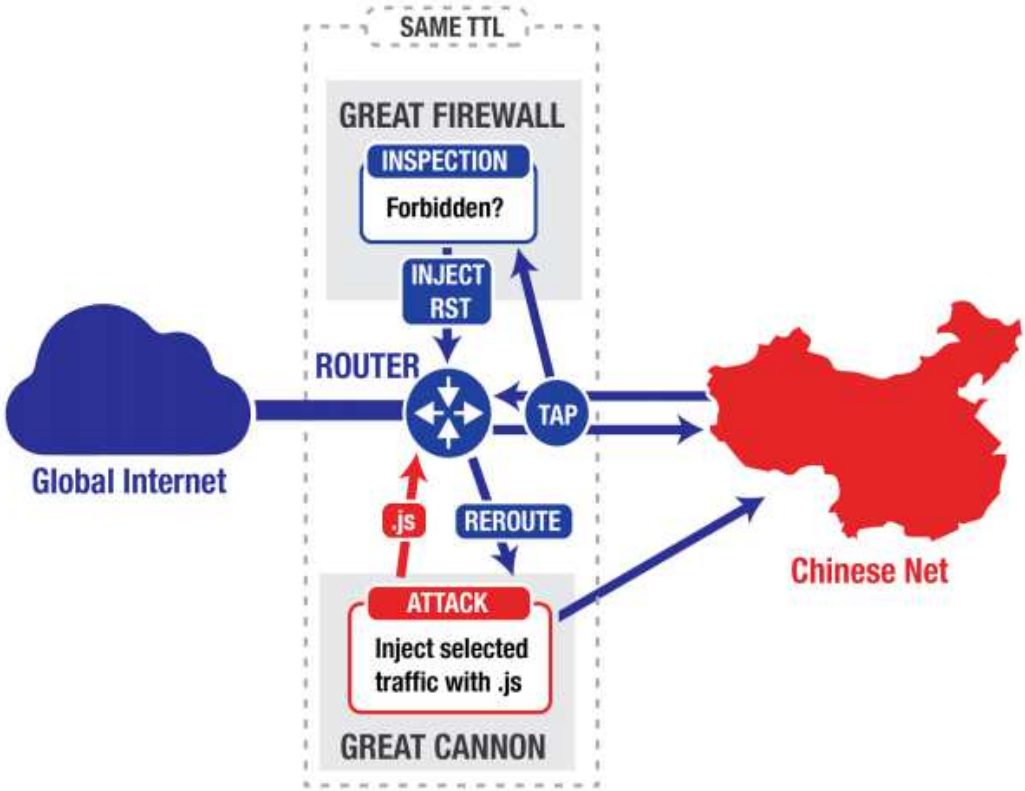

Figure 7. The Great Fire Wall of China &China's DPI Policy

Another example, Iran, this country has used a DPI mechanism similar with China. Iran purchased DPI tools from NSN or Nokia Siemens Network production which operating DPI mecjhanism national wide. In USA, NSA plays dominant role in DPI mechanism. The US has ability or capability to monitor the global Internet access network, because internet traffic in the world is associated with a large number of US servers. In terms of cyber security, one of the easiest tools that can be used in DPI mechanism is the development of the SSL protocol or Secure Socket Layer. SSL is protocol used by public when accessing the https or website. Https is one of the SSL security protocol contributions that will coding / embedding the data received and sent over internet.Another application tool is Darknet or Dark Web or well known as TOR Browser or Darknet browser. This is an interesting apploication, it can create identity of the Internet users and, of course, also encode their data (see Fig. 8). TORis the US Naval Research Institute product.

Figure 8. Illustration of the Dark Net (Dark Web)

Another question is to learn how to act when the internet users becomes victims. There are Internet disconnection could contain information,if a single user calls someone, the ringing tone stops slowly or not smoothly when both sides have good call or good network service. In this case, if the network feels confused about it, it may be questioning the act of arrest that may be made by hackers or third parties. Therefore, we should pay attention to it, as it can also be a hacking act.Various techniques might prevent internet wiretapping, such as instantly changing phone number and also connecting with customer service reporting there is strange interference in communications you have made so you can report your phone number account to the operator to be reviewed. Perhaps the most perfect way is to restore phone number, where in some cases phone processor chipsare characterized by permanent codes that are manufactured and that technician cannot work correctly. It is important to know the internet sounding techniques and responses, and it is also important to raise awareness of all our communications through mobile phones or the Internet.

6. CONCLUSION

To conclude this papers, here are some recommendations:

- Firstly, law enforcement officials can use most efficient and efficient remediation technique in DPI for intelligence, surveillance and intelligence operations. It is necessary to take into account that DPI (Deep Packet Inspection) is used for special cases relating to unusual offenses such as terrorism, radicalism, fraud, propaganda, corruption, drugs, the Internet, eavesdropping and so on.
- Secondly, the law on internet eavesdropping should be able to handle proportionality and necessity basic principles to avoid human rights abuse, by collecting facts legally proven by court.
- Thirdly, in terms of Internet interception, eavesdropping or wiretaping Act must clearly firm Internet's tap activity, disable and record terminology, as well as the mounting technology used, borderline-less, state-less and time-less.
- Fourthly, in terms of cyber security, eavesdropping or wiretapping law can be combine with the cryptography law, to tackle criminals of extraordinary crime over the internet.

References

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), Pp. 544-559.

Book of Guido Gluschke, Prof.Dr. Mesut HakkiCasin, Marco Macori (Eds.) (2018). "CyberSecurity Policies and Critical Infrastructure Protection". Copyright © 2018 by Institute for Security and Safety (ISS) Press, ISBN 978-3-00-060505-5 (pdf).Institute for Security and Safety GmbH.David-Gilly-Str. 114469 Potsdam.Germany. 2018.

Guido Gluschke, Prof.Dr. Mesut HakkiCasin, Marco Macori (Eds.) (2018). Book of "CyberSecurityPoliciesandCriticalInfrastructureProtection".Copyright © 2018 by Institute for Security and Safety (ISS) Press, ISBN 978-3-00-060505-5 (pdf).Institute for Security and Safety GmbH.David-Gilly-Str. 114469 Potsdam.Germany.

Internet Browsing (2019). What is Eavesdropping, https://www.techopedia.com/definition/13612/eavesdropping, accessed on 28July 2019.

Internet Browsing (2019). What is Wiretapping, https://whatis.techtarget.com/definition/wiretapping, accessed on 29 July 2019.

Madhusanka LiyanageIjaz, et all. (2017). "Enhancing Security of Software Defined Mobile Networks". IEEE Journal. May 2017. IEEE Access Pp. (99). DOI: 10.1109/ACCESS.2017.2701416.

Peter M. Shane (2018). International Journal.NSA Surveillance: Security. Privacy. and Civil Liberty. Journal of Law and Policy for the Information Society. Volume 10, Issue 2. DOI:10.31228/osf.io/7mdyr. December 2018. accessed 19 July 2019.

Paramadina Foundation (2015). "BelajardariKasus Edward Snowden" (Learn from Edward SnowdenCase), http://paramadina.or.id/2015/04/20/belajar-dari-kasusedward-snowden/, accessed on 21 July 2019.

President Obama's International Strategy for Internet (2011). "Prosperity, Security, and Openness in a Networked World". May 2011.https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed on 1 August 2019.

Rafael Antonello, Stenio Fernandes, et all (2019). Conference Paper. Deep Packet Inspection tools and techniques in commodity platforms: Challenges and trends, Journal of Network and Computer Applications 35(6):1863–1878, DOI: 10.1016/j.jnca.2012.07.010. November 2012. Accessed on 15 July 2019.

Sueddeutsche (2019). "Panama Papers (the Secrets of Dirty Money)", http://panamapapers.sueddeutsche.de/articles/ 56febff0a1bb8d3c3495adf4/, accessed on 19 May 2019.

Xuran Li and Hong-Ning Dai and Qinglin Zhao (2014).Conference Paper.An Analytical Model on Eavesdropping Attacks inWireless Networks. IEEE International Conference on Communication Systems. DOI: 10.1109/ICCS.2014.7024861. November 2014. accessed on 14 July 2019.