Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection

Bakri Mat, Siti Darwinda Mohamed Pero, Ratnaria Wahid, Babayo Sule

Abstract--Cybersecurity is one of the recent areas of concern for national and global security in the 21st century. It is a required segment of security at individual, enterprise, national and international level both at public and private sector. The current economy in emerging economies is shifting towards digital activities and Malaysia is one of these economies. For a digital economy to flourish, there is a need for a secured cyberspace which is the essence of cybersecurity. This work examined the impact of a secured cyberspace or the role of cybersecurity in promoting digital economy in Malaysia through a trusted law for customers and enterprise. The issue of concern is the risk of vulnerability in cyberspace which means there is an existence of threats to cybersecurity. The work used a qualitative method of data collection and analysis. Data were collected from both primary and secondary sources and were analysed using content analysis where thematic analytical interpretations was used. The paper discovered that, the cybersecurity in Malaysia is less vulnerable and is satisfactory but still there exist threats and vulnerabilities which can affect digital trust and digital business. Therefore, it is recommended that the laws on digital trust and cybersecurity should be consolidated and public awareness should be intensified to minimise the risk and to prepare for future unforeseen.

Keywords: Cybersecurity, Digital Economy, Enterprise, Law, Risk.

I. INTRODUCTION

Cybersecurity is one of the major components aspects of national and international security today globally. The attempts to promote international security at the global level compelled world governments to continue with the search for a better means of peace negotiation and conflict resolution (Wolfers, 1964). A shift in security and strategic studies by many scholars identified that there are two major typologies of security locally and internationally; the traditional and nontraditional security. Scholars (Buzan 1983, Leffler 1990, Johari 1997 and Buzan & Hansen 2009) argued that the previous emphasis on only traditional/military national and international security is no longer tenable within the discourse of security and strategic studies. There are other aspects of non-traditional/ non-military threats such as the polity, economy, environment, national cohesion, natural disasters such as flood and drought, energy security, food security should also be considered as areas of concern in security discourse at national and global level. Cybersecurity is one of the areas that recently fall within the category of non-traditional security threats nationally and internationally in recent times.

Cybersecurity is an area of concern for policymakers, analysts and international agencies (Fischer, 2009). Cybersecurity posts a security dilemma for national and international governments in terms of how to secure their domain from the threats of cyberattacks which is difficult because of anonymity and borderless nature of the phenomenon (Buchanan, 2016). The threats of cyberattacks has been affecting individuals, national government, world government globally, private enterprises and public enterprises alike. This phenomenon of cyberthreats affects particularly the new emerging economies which have their economy shifting towards digital economy and digital business activities (Antonucci, 2017).

Malaysia is one of the countries that is faced by the threats of both traditional (military) and non-traditional (non-military) threats at national, regional and global level (Saravanamuttu & Beng 2010 and Abdullah 2011). Malaysia is becoming a global economic force which is gradually having her economy moving into a digital arena and the risk is the fact that any digital economy is faced by threats and vulnerabilities of cyberattacks and cybercrime where hackers and cyber criminals are engaged in attempts to intrude into the vital information of government and private businesses for internet fraud (Abdul Rahim, 2017).

This study is an attempt to examine the role of cybersecurity in promoting digital economy in Malaysia using a trusted law for customers to secure their confidence and enterprise to protect them from cyberattacks and cybercrimes that will harm their business activities. In doing so, some related literature on the field were critically reviewed which enabled for an identification

Revised Manuscript Received on May 23, 2019.

Bakri Mat, International Affairs Management, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Siti Darwinda Mohamed Pero, International Affairs Management, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Ratnaria Wahid, International Affairs Management, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

Babayo Sule, Political Science Department, Federal University, Kashere, Gombe, Nigeria

of the research gap and contribution to knowledge because this area of study was not given adequate attention by scholars.

II. MATERIALS AND METHODS

The research adopted qualitative method of data collection and analysis. Qualitative research is the use of both primary and secondary data in obtaining information for research using specific techniques suitable for the type of research in question and the nature of the environment for conducting the research (Sharan, 2002, Sekaran & Bougie, 2013 and Creswell, 2014). Qualitative research uses words as data collected and analysed using all forms of data analysis. The term qualitative research refers both to techniques of data collection and analysis and a wider framework for conducting research or paradigm (Creswell, 2014:7). Paradigm here refers to the beliefs, assumptions, values and practices shared by a research community (Creswell, 2014:8).

The primary data was collected by conducting an interview with some selected senior officials from selected categories. The first category is high-ranking officials from Malaysia's national security sector from Ministry of Defense who deal with cybersecurity issues where two of them were interviewed. The second category is from Malaysia's National Communication Commission (MCMC) where a senior official that handles digital aspects was interviewed. The third category is selected from the private digital business sector where two senior officials was interviewed. The fourth category was selected from the Malaysian Administrative Modernisation and Planning Unit (MAMPU) where a senior official was interviewed. The fifth category is the academicians where two experts Professors were interviewed from a reputable Malaysian University one of them an expert in national security and strategic studies while the other an expert in the field of computing and digital system.

The other primary sources consist of governmental documents such as Malaysia's official document on national security (Keselamatan Negara) and Malaysia's national security core values as well as Malaysia's national security plan on cybersecurity. The secondary source is the use of available literature on the subject matter of study and documented materials from Perpustakaan Sultanah Bahiyah, Universiti Utara Malaysia; Perpustakaan Tun Sri Lanang Universiti Kebangsaan Malaysia; Perpustakaan Institute Strategic and International Studies (ISIS- Kuala Lumpur) and Centre for Cybersecurity Malaysia. These materials involved books, journals, articles, newspapers, magazines and internet sources.

The data obtained from the primary sources and secondary sources were coded, presented and analysed using content analysis. The data analysis involved the use of content analysis and its pertinent here to explain in clear terms what content analysis is. The data obtained was discussed and analysed using thematic analytical interpretations together with the existing literature and the application of the theoretical framework adopted in the research.

III. LITERATURE REVIEW

In this section, relevant existing scholastic views on the subject matter of study were examined and discussed critically including the concept and issues in cybersecurity and digital economy or digital services. This has been discussed below.

Concept and Issues in Cybersecurity

Cybersecurity is presently an area of concern for national governments in order to ensure a well-protected security and a cyberspace environment for a safety business and protection of critical national Infrastracture. Cybercrime is now one of the major issues of policymaking at national and global level because of its threats globally. A good example is that cybercrime cost $1 trillion USD globally in 2013 and it is still ongoing. Funds are stolen, vital information are hacked, critical infrastructures are attacked and rendered incapacitated and individuals are vulnerable and at risk of being targetted withier private communication and information by the criminals (Mowbray, 2013:4).

The world today survives on digital or internet communication where a large amount of information is stored and transferred. But, this practice is done at a greater risk because an unwanted target or fraudsters can access such data and used it negatively as against the ethics of the government, private organisations or a breach of personal privacy. This is where cybersecurity is most needful. Cybersecurity is not only an issue of protecting criminals from hacking government and business information but it is also the need to protect and secure the digital environment from risks and threats of vulnerabilities which may affect government functions, private business and particularly digital economy (Meeuwisse, 2015:8).

Cybersecurity is basically involving information categorisation, integrity of confidential data and permission, defense, devices, services, networks and control systems including physical, technical, procedural and legal. Cybersecurity is a new area of security study which is not fully understood in terms of its nature, dimension, trends of occurrence and other issues related to it and this explains why it is difficult to handle. Cybersecurity is mainly concern with the cyberattacks because the attackers use an entry point in the network services to cause damages such as infection, persistence, communication and control. Cybercrime is borderless and can be perpetrated by criminals from within, outside, terrorists, organisations and even enemy government (Meeuwisse, 2015:8).

Cybersecurity is the activities, laws, policies and responses made by policymakers to identify vulnerabilities and risks of cyberthreats from protected gadgets such as computers owned by the governments, private organisations, business enterprises and individuals and vital information that are stored

against the undesired elements or targets. Cybersecurity refers to a set of activities and other measures intended to protect from attacks, disruption or other threats from of computers, computer networks, related hardware and devices software and the information they contain and communicate including software and data as well as other elements of cyberspace. It also includes the state of being protected from such threats and the broad field of endeavour including research and analysis aimed at implementing and improving those activities and quality. The major weaknesses in Cybersecurity consist of service disruption, theft of assets and control (Fischer, 2009:28).

There is increasing concern among government officials and industry management regarding the potential for a cyberattacks on the national critical infrastructure including its control systems. There are identified multiple sources of threats to nation-states critical infrastructure. Nation-states engaged in information warfare, domestic criminals, hackers, virus writers and disgruntled employees in an organisation. Attacks on cyberspace can lead to denial of services, exploitation of tools, logic bombs, infusion of virus, war driving and zero-day exploit. Cybersecurity is a deliberate synergy of technologies, processes and practices to protect information and the networks, computer systems and appliances and progress used to collect process, store, and transport that information from attack, damage and unauthorised access. It is viewed as a holistic set of activities that are focused on protecting an organisation's vital information. Cybersecurity includes the technologies employed to protect information (Norwood & Catwell, 2009:6).

Cybersecurity is an issue of much concern because the threats emanating from cyber affect both individuals and governments in addition to organisations. A good example is threats to personal privacy of individuals such as internet fraud and theft. At the organisational level, it may include employee sabotage and attacks on infrastructure as well as malicious hackers and industrial espionage. At the governmental level, it may include spy from other states, attacks on critical infrastructures, hacking vital governmental information and data and preventing normal functions of governmental assets (Rittinghouse & Hancock, 2003:1).

Cybersecurity involves prevention of vulnerabilities in information at personal, organisational and governmental level. The nature of vulnerabilities in information systems are risks in hardware, risks in software, risks in people, risks in computers, risks in cyberspace and risks in insurance in cyberspace. Vulnerabilities at individual level involve trust, ethics, communication, intelligence, courage and limitations. At the organisational level, the vulnerabilities involve human factors, security services, external technologies, wireless networks, and fidelity, worldwide microwave access and cloud computing. At the level of government, the vulnerabilities include organised criminals, nation-states, critical infrastructures, confidential policy documents and classified data. Thus, it is good to device means of cyber defense. Cyber defense can occur through file protection application, PC performance applications, protection tools and email protection as well as cybercrime laws and policies (Kostopoulos, 2013).

Laws and Policies on Cybersecurity

There is still the existence of gap in cybercrime and cyber law as cyber laws are still poorly construed or simply do not apply to the types of crimes to be investigated. Also, many cybercrime laws differ from one state to another and from one country to another. The laws are not universal in application and nature (Reyes, O'Shea, Steele, Hansen, Jean & Ralph, 2007).

Anti-hacking laws are intended to help promote Cybersecurity. However, some critics argue that these laws are outdated and not only fail to help protect private and government computers but also penalize individuals for conducting entirely legitimate activities such as cybersecurity research. Cybersecurity law is often associated with punitive measures and also protective measure such as Government Surveillance Laws and privacy laws (Kosseff, 2017). The issue of how the nation-states respond to cyber attacks reflects the essence of international law especially predicated along the nation-states' rights to defend itself when attacked in accordance with Article 51 of the UN Charter. Regarding cybersecurity, the intended target is the nation-state's internet infrastructure. It is for that reason that the relationship between cybersecurity and international law was established considering the fact a cyber hacker may also be considered a legitimate target in the context of operational counterterrorism is warranted (Guiora, 2017:63).

The convention on cybercrime is the only international agreement in existence at global level signed by some European member countries in the area of cybercrime. It is also open for membership entrance for example; it was signed by United States, Canada, Japan and Australia. The convention has three key divisions, substantive law, procedural requirements and international cooperation. The convention identified four main categories of substantive offence to have included: i. offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices; ii. Computer-related offences such as forgery and computer fraud; iii. content related offences, in particular the production, dissemination and possession of child pornography and iv. Offences related to infringement of copyright. The convention also addresses the procedural aspects of cybercrime as follows: i. expedited preservation of stored computer data; ii.Expedited preservation and partial disclosure of traffic data; iii. Production orders; iv. Search and seizure of stored computer data; v. real-time collection of traffic data and vi. Interception of content data. Finally, the convention contains provisions related to international cooperation which are: i. extradition; ii. Mutual assistance and designation of a 24/7 network contact (Maurushat, 2013: 36).

The need for policies on cybersecurity is anchored on the notion of the shift in global governance towards e-governance and its security implications. The 2009 attacks on South Korea and United States of America present a good case for concern in this perspective. Thus, a good policy on cybersecurity should target a global approach in order to ensure collective security (Andreason, 2012:77). The dilemma of cybersecurity issues is the tyranny of geography. These include diffusion of responsibility between government and organisations, civil liberty and private issues, the public-private conundrum and the people issues (Andreason, 2012:78). Cybersecurity laws should target the protection of four major issues. The first is personal and family protection which consists of stocks, bonds, bank account and credit card, Medicare accounts, protection of desktop computers and Wi-Fi, personal cell phones and family records. The second aspect involves cybersecurity policies for smart phones and free Wi-Fis which through mobile phone security and access. The third aspect is protecting vital infrastructure through application of satellites with cybersecurity implications. The fourth is strict government regulations and monitoring of cyber activities (Pelton & Singh, 2015).

The problem with legal settings on cybersecurity is privacy issue. Privacy concerns and law enforcement is a major concern here. There is a conflict between information technology, privacy and national security. The legal limitations on national security data gathering and tensions between privacy and national security, law enforcement, national security and individual privacy affect policies on cybersecurity and they must be taken into consideration when formulating the policies to strike a balance between the threats and security of the country concern (Waldo, Lin & Millet, 2007).

Cybersecurity policies and laws emerged as a result of detrimental activities and dubious acts of occurring in cyber space. The United Nations developed some cybersecurity policies to cater for international security which includes Internet Governance Forum (IGF) and the ITU as two multinational stakeholder advisory entities operating under the UN umbrella. The membership includes academicians, private industry, government officials, general public, advocacy groups and others to recommend best industry practices to be cyber safe and keeping the internet borderless and accessible to all global citizens (Pelton & Singh, 2015).

Digital Economy

A large number of business today adopted technology for their business using various means of innovation and advancement towards customer services and operations. Those enterprises that adopted technology in their business operations prosper more currently and have their businesses operated easier than before (Shalhoub & Al Qasimi, 2010). Enterprises face an unauthorised use and attacks which are malicious in nature such as theft, destruction of intellectual property, abuse by insiders and illegal use of information which tantamount to loss of data reliability and confidentiality. These cyberattacks affects trust of enterprise and users or customers in terms of using internet for transaction (Shalhoub & Al Qasimi, 2010).

Trust in the use of information security and the use of cyber space. Trust is a condition of evolving and developing positive confidence about another party's intention, activity and service as well as its reliability most especially when a risk is involved. Trust at organisational level or enterprise is about the confidential and secured benefit that an individual is expecting in his/her relationship with the organisation. The position of trust in the use of internet for conducting business activities cannot be over-emphasised and must be given adequate attention due to the shifting nature of businesses globally into a digital space. There are serious challenges to digital economy or businesses including separation of the buyer from the seller physically, separation of the buyer from the product, distance in the environment and the risks of cybercrimes. Enterprises must find ways of initiating and developing this cyber relationship and the best way of doing it is through trusted digital space (Shalhoub & Al Qasimi, 2010). The distance and lack of physical contact between the business and the customer made it necessary for the business to ensure that they promote digital trust.

The need for developing this digital trust between enterprises and customers is because of the evolving relationship between the two currently. Customers are becoming connected to internet businesses today at a rapid pace and the speed of internet businesses is becoming faster and conventional globally which made the internet-based businesses with ultimate chances in e-commerce. Business conducted online today will in the near future dominate the commercial activities in developing economies. But, for such e-businesses to thrive and progress, consumer loyalty is necessary and this can be achieved through a digital trust where the customers can trust confidently the services and businesses partners with less risks (Shalhoub & Al Qasimi, 2010).

Digital economy has the advantage of providing 24/7 services conveniently within the bedroom of a customer with less difficulty. A study revealed that more than 42 % of businesses were conducted online globally in 2017 (Choi, 2017).

In Malaysia, the digital economy is boosting and improving the economy to advance level. Malaysia's digital economy is set to contribute 20 % of the Nation's GDP in the year 2020 more than 18.2 % in 2016. In addition, Malaysia has set up a digital free trade zone (DFTZ) located near the Kuala Lumpur International Airport (KLIA). The Prime Minister Tun Najib Razak was reported in 2017 to have said "The Malaysians have embraced the internet economy and e-commerce in a big way. We are now leading the e-commerce in the region generating revenue of $2.3 billion in 2015.

With the launch of the world's first largest free digital trade zone, Malaysia will serve as a regional e-fulfillment centre and will also become the regional hub for SMEs, market places and mono brands (Tan, 2017).

But a digital economy in Malaysia is more than just providing a convenient platform for Malaysian enterprises to transact businesses, it must include protecting and securing the people in a safer environment. Public safety should be considered in digital transformation. New technologies such as advanced CCTV should be put in place for safety and security. The Police Force should be improved too with digital training. Central to Malaysia's digital economy is the improvement in broadband infrastructure. In this regard, the government in 2017 planned to raise broadband speed to 20Mbps in rural areas and 100Mbps in urban areas by 2020. An amount of RM1 billion (US240. 5 billion) was earmarked in the 2018 budget to improve broadband connectivity in the east Malaysian states of Sabah and Sarawak (Tan, 2017).

Thus, it can be summarised from the above that the future of the world economy is entirely moving towards the digital economy in the nearest time and Malaysia is one of the destination for the flourishing of the digital economy especially with a serious effort from the government in fostering such development rapidly. What is the most important issue to consider is how to secure a trusted digital economy and the trust of the enterprises themselves and their customers in the process.

IV. DISCUSSIONS AND FINDINGS.

In this section, important that were discovered by the research were presented and discussed thematically with the existing literature and framework of analysis to arrive at conclusion, contribution and policy recommendation for future implication.

Trusted Digital Economy in Malaysia: Policy Response and Implications

There are many views from the informants on the nature of trusted digital economy in Malaysia and the various methods that can be followed to achieve such a trusted digital economy in Malaysia. Their views were summarised and presented below for discussions. One of the informants from the business sector narrated that "One is security actually security and number two agent of change also agent of inclusion in service. So when you talk of internet programmes of course there is a lot of programme we have programmes to boost internet border force online products but there are few strategies we have. Number one I will say digital technologies we have the devices so that. Number two there is also the data so we talk about the data the electronic payment and other online transaction so they are pushing so hard there are many categories for the financial sector that is why you will change your card everyday even though that was a painful exercise mind you but to be at the safer side because of this it is done. And then there is a trust and associate player and thus there are two elements number one there is a promise and then there is access".

He further added that:"So on the left there is a promise on the digital economy. If we do not get people to get access to these digital services the likes of MAMPU what they will do in their jurisdiction that means it will be leading to digital trust because this people will not get included in the access as everybody else has phone in his hand. So, number one is to provide education for Malaysians we have mentioned before we talk about all digital services online we talk about businesses we talk about e-commerce we talk about acquiring information these information I think is good in learning for the future. I think if we look at the few transformational plan that has been actually plan by some ministries for example MOH".

In addition, he suggested the impact of the digital economy in the following statement:" Number two once you have the digital ID in place it will transform service delivery and it will become a reality. Number three a population explosion like India which has 1.1 billion citizens they will simply introduced digital implementation so what they have done is to enroll 1.1 billion of their citizens May this year so imagine these numbers and what if we can utilize this ID and open bank account online in the country wherever you are in India you can open bank account online and as you know bank account in India you will need to have an element of KYC bringing your documents right so once you open a digital ID once you have your digital ID you do not need the elements of KYC again and again and again. That means in India the earlier you have a digital ID you can open a bank account you can achieve government services you can achieve businesses you can achieve e-learning all from your home comfortably. So you see generally that is what I am trying to say for the first round digital ID education we want to introduce".

In another different view from another interviewer, trusted digital economy in Malaysia is perceived to have been achieved through:" So our strategy is one of as I mentioned earlier public sector approach focusing on sustained economic growth, social development and environmental protection and to actualize this strategy we have a number as I mentioned earlier government projects as you see in the slides government online services, national registry and records sector and the government big data and open data to the programmes and the government data optimization programme towards digital trust we all know about this.

This is to get us in strategising for cost saving to the government to increase for innovation and get digital economy by our services".

Another informant in his view suggested that for a trusted digital economy, there is need for: "an enlightenment on the risks and vulnerabilities of cybersecurity on the parts of the people and the businesses themselves as well as the government. The academia should intensify their efforts in doing so in order to ensure that people are given enough awareness on their personal transaction on the internet.

Another informant suggested that:" The digital economy in Malaysia is doing good on the record. Malaysia was remarkably third in the global ranking of Cybersecurity Index in 2017 after Singapore and Us. Hopefully, Malaysia can overtake US next year. There are different agencies that are working busy towards a trusted digital economy and a safer cybersecurity environment in Malaysia such as the Malaysian Communication and Multimedia Commission (MCMC), Cybersecurity Malaysia (CSM), Majlis Keselamatan Negara, Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), National Cybersecurity Malaysia (NACSA) and academicians in the area of specialisation of computing and networking. These agencies work hard independently but coordinately in ensuring a secured cyberspace in Malaysia and a trusted digital economy. They are really succeeding but there is need to do more especially in deterrence and rapid response in case of any attacks".

V. FINDINGS

The study identified the following findings:The digital economy in Malaysia is gaining a greater strength gradually contributing by next year about 20% of the country's total GDP and the government is making a serious effort in providing billions to boost internet services to facilitate digital businesses which made the country the highest in the region in terms of digital economy and one of the best performing globally.

The study also discovered that the cybersecurity in Malaysia is satisfactory the multi-approach by different agencies such CSM, MAMPU, MCMC, NACSA and Keselamatan Negara towards a secured cyberspace and a trusted digital environment that will facilitate businesses and individual privacy and safety in the internet services.

The study also found that there might be threats, risks and vulnerabilities in the cyberspace which can affect people's trust in the digital economy and there is need for the enterprise and the government as well as individuals to take safety measures to ensure a safer digital business and internet services.

VI. CONCLUSION AND RECOMMENDATIONS

The paper concludes that cybersecurity is one of the modern challenges of national and international security from the perspective of non-traditional security discourse. The study also concludes that digital economy is now the most dominant business transaction that is growing faster in the commercial sector across the globe and particularly in Malaysia where more than 40 % of the business transactions in the country are today conducted digitally and the future of businesses in Malaysia relies on digital economy. The paper also concludes that for a reliable digital economy to be on ground or in place in Malaysia there must be trusted digital space among the enterprises, customers, public sectors and individuals at their different level. This trusted digital economy can be achieveand sustained through an improved law and policy on cybersecurity which is currently in existence in Malaysia but it needs more consolidation. The study therefore recommends that:

1) There is need for a cooperation between the public and private sector towards a secured cyber environment in Malaysia;
2) The business enterprise should invest in research in search for a means of guaranteeing trust in the digital business and fostering of confidence in their customers;
3) There is need for massive public awareness and enlightenment campaign on the risks, threats and vulnerabilities on cyberspace to minimise the risk of compromise and attacks and
4) The agencies responsible for cybersecurity safety in Malaysia such as CSM, MCMC, NACSA, MAMPU etc. should increase their vigilance and coordination towards providing a better environment for cyberspace that is safer and trusted as well as reliable.

ACKNOWLEDGEMENT

This research was supported by the Ministry of Education under the FRGS grant Code S/O: 13809. We thank our colleagues from Universiti Utara Malaysia who provided insights and expertise that greatly assisted the research, although they may not agree with all of the interpretations of this paper. We would also like to show our gratitude to everyone for sharing their pearls of wisdom with us during the course of this research, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

1. Abdullah, K.B. (2011). Emerging Threats to Malaysia's National Security. Journal of Policing, Intelligence and Counter-Terrorism. 5(2), 55-70.
2. Abdul Rahim, N.B. (2017). Malaysia's CyberDefence Capabilities to Counter Cyberthreats:Protecting Critical National Information Infrastracture (CNII). Masters Thesis Submitted To the School of International Studies, College of Law Government and International Studies, Universiti Utara Malaysia.
3. Andreason, K. (2012). Cybersecurity: Public Sector Threats and Responses. London: Taylor &Francis.
4. Antonucci, D. (2017). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. New Jersey: John Wiley & Sons.
5. Buchanan, B. (2016). The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. New York: Oxford University Press.
6. Buzan, B. (1983). People, State and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Sussex: Great Britain.
7. Buzan, B. & Hansen, L. (2009). The Evolution of International Security Studies. New York: Cambridge University Press.
8. Choi, K. (2017). 99 Facts on the Future of Business in the Digital Economy 2017. Retrieved at https://www.slideshare.net/sap/99-facts-on-the-future-of-business-in-the-digital-economy-2017).
9. Creswell, J. W. (2014) Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research. Edinburgh: Pearson Inc.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

10. Fischer, E.A. (2009). Creating a National Framework for Cybersecurity. An Analysis of Issues And Options. New York: Nova Science Publishers.
11. Guiora, A.M. (2017). Cybersecurity, Geopolitics and Law. London: Routledge.
12. Johari, J.C. (1997). International Relations and Politics (Theoretical Perspectives). New Delhi:Sterling Publishers.
13. Kosseff, J. (2017). Cybersecurity Law. USA: John Wiley & Sons.
14. Kostopoulos, G.K. (2013). Cyberspace and Cybersecurity. London: Taylor & Francis.
15. Leffler, M.P. (1990). National Security. The Journal of American History. 77(1), 143-153.
16. Maurushat, A. (2013). Disclosure of Security Vulnerabilities: Legal and Ethical Issues. Berlin: Springer.
17. Meeuwisse, R. (2015). Cybersecurity for Beginners. Canterbury: Icutrain Ltd.
18. Mowbray, T.J. (2013). Cybersecurity: Managing Systems, Conducting Testing, and InvestigatingIntrusions. Indianapolis: John Wiley & Sons.
19. Norwood, H.T. & Catwell, S.P. (2009). Cybersecurity, Cyberanalysis and Warning. New York:Nova Science Publishers.
20. Pelton, J.N. & Singh, (2015). Digital Defense: A Cybersecurity Primer. USA: Springer.
21. Reyes, A. O'Shea, K. Steele, J. Hansen, J.R. Jean, C.B.R. & Ralph, T. (2007). Cybercrime
22. Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors. Massachusetts: Elsevier.
23. Rittinghouse, J.W. & Hancock, W.M. (2003). Cybersecurity Operations Handbook. Amsterdam: Elsevier.
24. Saravanamuttu, J. & Beng, O.K. (2010). Malaysia. In Severino, R.C. Thomson, E. & Hong, M. (Eds.) Southeast Asia in a New Era: Ten Countries, One Region in ASEAN (pp.111-132).Singapore: Institute for Southeast Asian Studies.
25. Shalhoub, Z.K. & Al Qasimi, S.L. (2010). Cyber Law and Cyber Security in Developing and Emerging Economies. Northampton: Edward Elgar.
26. Sharan, M.P. (2009) Qualitative Research Method San Francisco: John Wiley & Sons.
27. Tan, A. (2017). Deputy prime minister outlines Malaysia's digital efforts, noting that the digital economy will account for one-fifth of the country's GDP by 2020. Computerweekly.com. Retrieved from https://www.computerweekly.com/news/450430259/Malaysias-digital-economy-on-track).
28. Waldo, J. Lin, H.S. Millett, L.I. (2007). Engaging Privacy and Information Technology in a Digital Age. Washington: The National Academy Press.
29. Wolfers, A. (1964). Discord and Collaboration: Essays on International Politics. Baltimore: The John Hopkins Press.