SEYBOLD Report
ISSN: 1533 - 9211

CONFIGURING CYBER ESPIONAGE RISKS VIA THE RISK SOCIETY-CYBER SECURITISATION THEORY

W.R, Wan Rosli[1]**, Z, Hamin**[2]**, S., Kamaruddin**[3] **and A.R., Abd. Rani**[4]

[1, 2, 4]Faculty of Law, Universiti Teknologi MARA, Shah Alam, 40450 Selangor, Malaysia.

[3]Faculty of Management and Economics, Sultan Idris Education University, Tanjung Malim, Perak, Malaysia.

Email: *[1]rosalili@uitm.edu.my; [2]zaiton303@uitm.edu.my; [3] saslina@fpe.edu.my; [4]ridhwanrani@uitm.edu.my

ABSTRACT: Of late, cyber or virtual attacks by non-state and state-backed actors against government websites, public and private networks, confidential networks, and individuals have become more and more rampant. Such phenomena highlight the risk of being connected to the Internet, primarily where the environment of cyberspace facilitates anonymity. The emergence of cyber espionage to spy on the government, public, or private sector acts as a visible threat to national security. The prevalent theoretical approaches adopted to understand cyber espionage is the Risk Society Theory (RST) and the Cyber-Securitisation Theory (CST). However, on their own, these two theories are deficient in that RST relies on the risks and insecurities that come with modernisation, and CST only focuses on the transformation of a domain into a matter of national security. Given these problems, this paper aims at examining each model and expanding and integrating the RST and CST, which would mitigate the understanding of cyber espionage and modalities to prevent such crime. This paper adopts a qualitative methodology, of which the primary data is generated from semi-structured interviews with relevant respondents. The data triangulation is obtained from experts at two relevant ministries. The secondary data are the relevant cyber law, the Penal Code, books, academic journals, online databases and library-based sources. The findings suggest that the risks of cyber espionage are often manufactured by the victims, who may be able to manage and mitigate such risks if integrated with the cyber securitisation model. The findings have significant implications not only for the stakeholders including the policymakers and law enforcement but also for individual responsibility of corporate entities and computer users to protect themselves against such crime as they are becoming new actors or new sites of authority in the information era.

KEYWORDS: *Cyber Espionage, Risk, Risk Society Theory, Cyber Securitisation Theory, Cybersecurity*

1.0 INTRODUCTION

Since the past decade, the world has become inextricably linked and dependant on the Internet. In Malaysia, the percentage of Internet users in 2019, mainly social media users, has increased by up to eighty-six per cent from seventy-three per cent in 2018 (MCMC, 2020). It is a truism that the Internet notably works as a double-edged sword where cyber-attacks provide non-state and state actors considerable opportunities to operate on a bigger scale with more flexibility.

The benefit of using the Internet to stage an attack is the avoidance of the need for physical injury and the ability to be in various locations at the same time (Wan Rosli, Kamaruddin, Hamin, 2020).

Cyber espionage or cyber spying is one of these attacks or cybercrimes that is getting more sinister than previously. Spying or utilising spies to gather information about the plans and operations of a foreign government or a competitor company is referred to as espionage (Demarest, 1995). Although state-to-state espionage is not a new phenomenon, the globe has moved into a whole new arena of spying or cyber espionage in the previous few decades (Rubenstein, 2014). In recent years, such crimes have included the use of information and communication technology (ICT) by individuals, groups, or businesses for financial or personal advantage (Maras, 2016). According to the United States Army Cyber Operations and Cyber Terrorism Handbook (2006), cyber espionage is a type of cyber warfare that includes computer network attacks such as data disruption, damage, or erasure. Espionage can take many shapes. Traditional espionage refers to a government's attempt to obtain secretly classified or otherwise protected information from another country (Setiawan & Heriyanto, 2020). Economic espionage refers to a government's attempt to get trade secrets from overseas private companies without their knowledge. "Corporate espionage" or "industrial espionage" is the illicit acquisition of a firm's trade secrets by a company with no government involvement (Fidler, 2013).

In a global context, the existing literature on cyber espionage demonstrates that such crime occurs when the spies are armies of nefarious hackers from around the world who would use cyber warfare for economic, political, or military gain (HOre et al., 2021, Patterson & Hanley, 2020, Wangan, 2015, Skinner, 2013, O'Hara, 2010). According to research on cyber espionage, culprits are usually highly valued hackers with the technical skills to shut down anything from government facilities to financial systems or utilities resources (Rodricks, 2020, Hansen, 2020, Reveron, 2012, Deibert et.al, 2009). The new rising threat of cyber espionage is also impacting the economic and political interactions between nation-states, as well as changing the nature of modern conflict, according to the literature. As a result, despite the benefits of contemporary technology, there are a slew of new issues to contend with (Jalali, 2021,Nardi, 2020, Baderna, 2019, Dun Cavelty, 2013). However, according to Fouad (2019), most cybercrimes, particularly cyber espionage, are policy-driven and under-theorized. In addition, previous research has focused little on the most effective model or theory for comprehending such crimes.

Extant literature in the Malaysian context revealed that Malaysia is one of the top ten riskiest countries for cyber-attacks (Khan, 2020, Ahmad, 2016, Borneo Post Online, 2013). In recent months, it has come to light that Malaysia has been the subject of cyber espionage activities aimed at government officials and linked to Chinese hackers (CyberSecurity, 2020, Khan, 2020). In the first six months of this year, 9,857 cases of cyber-crime were recorded, with 7,801 of them being solved and 3,385 people being arrested (CyberSecurity, 2020). The losses totaled RM1.115 billion last year, with 8,920 of the 11,543 recorded cases being investigated and 3,712 persons being arrested (CyberSecurity, 2020). The majority of the local literature focuses on how cybercrime affects various industries (Abd. Jalil et.al, 2020, Perumal et.al, 2018, Teoh, 2017). However, there is a scarcity of local literature on cyber espionage in general, and particularly on the theories that might be used to analyse such crimes.

As previously noted, recent literature on cyber espionage focuses mostly on the hard method, which is law-oriented, and as a result, such crime is under-theorized and lacks the soft approach (Fouad, 2019). Furthermore, insufficient attention has been paid to the ideas that support our understanding of such acts in the past. The Risk Society Theory (RST) and the Cyber-Securitization Theory (CST), which work in different ways, are two existing ideas that can be used to comprehend cyber espionage. Given the insufficiency of these two theories in describing cyber espionage on their own, this study will propose combining the RST and the CST to better understand cyber espionage and the mechanisms for preventing it.

The first part of the paper seeks to discuss recent cyber-espionage incidents briefly, followed by the second part which explains the legal landscape or criminalisation of such crime in Malaysia. Whilst the third part discusses the Risk Society Theory, the fourth part explains the Cyber Securitisation Theory. This is followed by the fifth part which attempts to merge both the theories in explaining such crime. The last part concludes this paper.

2.0 CYBER ESPIONAGE INCIDENTS

According to current research, the most vulnerable industries to cyber espionage include public administration, manufacturing, and education (World Economic Forum Global Risks, 2020, Nardi, 2020, Perlroth, 2019). There have been numerous reports of cyber espionage. In 2019, for example, Chinese and Iranian hackers targeted US government agencies (WEF, 2020, Spataro, 2019, Caravelli, 2019). Both the Iranian and Chinese governments and corporations are aggressively attacking US government institutions and enterprises. These attacks, according to cybersecurity experts, are a result of Trump's departure from the Iran nuclear deal and the trade battle with China (WEF, 2020, Herrmann, 2019). China, Iran, North Korea, and Russia are the country's top cyber foes, according to US intelligence leaders in January 2019. These countries are associated to cyber-espionage actions in the United States, such as stealing information to influence populations or disrupt key infrastructure (Caravelli, 2019, Paterson & Hanley, 2020). The Iranian hackers' goals, according to the study, were to gather intelligence and position themselves for future cyber operations. (Perlroth, 2019, Caravelli, 2019, Kittichaisaree, 2017, Reveron, 2012; Perlroth, 2019, Caravelli, 2019, Kittichaisaree, 2017, Reveron, 2012).

A dispute emerged in late February 2013 after a US cybersecurity firm produced a study stating that the Chinese military was using cyber technology to steal trade secrets from Western corporations. Similarly, the New York Times revealed in January 2013 that it had been hacked from China, prompting accusations that other publications had been hacked as well. The United States is the target of cyber-espionage, according to a National Intelligence Estimate released on February 10, 2013, with China as the country most aggressively attempting to penetrate the computer systems of American businesses and institutions in order to gain access to data that could be used for economic gain (Fidler, 2013, Libicki, 2016). The infamous Estonian cyber-attacks appeared to be planned informally on Russian online chat rooms far earlier in 2007, and the Russian authorities made dire statements about the Estonian government while appearing uninterested in apprehending the hackers (Ilves et al., 2016). Even if cyber espionage norms existed, they would be meaningless because of the difficulty of international attribution.

3.0 THE CURRENT LEGAL LANDSCAPE OF CYBER ESPIONAGE

The goal to combat cyber espionage is met with a lack of international law on espionage and economic espionage in the global scenario. Although a victim country may claim that spying breaches sovereignty and non-intervention principles, state practise has accepted state-sponsored espionage to the point that such allegations are not serious (Longobardo, 2020). Despite the fact that cyber espionage is sometimes referred to as "cyber-attacks" and "cyberwar," no nation considers any kind of cyber espionage to be a prohibited use of force (Longobardo, 2020). Other international treaties that deal with espionage, such as those on armed conflict and diplomatic relations in times of peace, do not prohibit or severely restrict espionage or cyber espionage (Chesterman,2013: Filder,2013). Because espionage is lawful, the situation of espionage is rather unsatisfying. After all, it isn't expressly forbidden. This position appears to have been acknowledged in the landmark Tallinn Manual (a NATO publication discussing the application of international law to cyber-attacks), which argued that cyber espionage is not inherently illegal. This is akin to the Lotus judgement of 1927, which held that anything not expressly prohibited by international law is legal (Robinson, Jones & Janicke, 2015). Cyber espionage rests on this shaky thread. Meanwhile, the international norms controlling cyber espionage will remain void. Because international law for new technology evolves by analogy, it's unsurprising that the law on cyber espionage is a quagmire (Skinner, 2013; Barnes, 2018, Longobardo, 2020).

The Communication and Multimedia Act 1998 (CMA 1998), the Computer Crimes Act 1997 (CCA 1997), the Penal Code, and the Security Offences (Special Measures) Act 2012 are among the traditional and computer-related laws that can be used to prosecute cyber espionage in Malaysia (SOSMA 2012). Sections 234 (1) (a) and (c) of the CMA 1998 prohibit the interception of any communication, and the content of communication may thus be used to prevent the transfer of information from one party to another in the case of cyber espionage. Section 234 (1)(b) can be utilised to prevent the public disclosure of any information gained through communication interception. Cyber espionage can also be prosecuted under sections 3, 4, 5, and 9 of the CCA. Section 3 of the CCA governs unauthorised access to computer materials, while section 5 of the CCA governs unauthorised modification of any computer's content. In both cases, the victim must submit to the police or the Malaysian Communication and Multimedia Commission (MCMC) for an investigation before being arrested and charged. According to the literature on SOSMA, it is a preventive statute designed to protect residents' lives and property. The Act establishes unique procedures for dealing with security offences and recognises the considerable threats that terrorism, sabotage, and espionage pose to internal security and public order (Dhanpal and Sabaruddin, 2017). Furthermore, Section 124M of the Penal Code specifies that anyone who commits espionage by any means, directly or indirectly, faces a life sentence.

4.0 THE RISK SOCIETY THEORY

Risk society, according to existing literature on RST, is a society that is increasingly focused with the future and safety, which generates a sense of risk. Beck (1998) describes risk society as a systematic approach to dealing with the hazards and insecurity that modernization has produced and created. Beck (1998) and Giddens (1998) look at the RST through the lens of modernity, which sees current society as far more dynamic than any earlier society and as living in the future rather than the past. Modernisation is also defined by Beck (1998) as surges of technical rationalisation and changes in employment and organisation, which involve changes in lifestyle and forms of love, societal features, and ordinary biographies. Given the reality and norms of knowledge, further changes include a shift in power structures and impact in the forms of political repression and participation. Giddens (1998) goes on to say that the hazards in modern societies increase as governance and technology control, as well as societal production and consumption systems, become more complicated.

Humans have always been subject to a certain level of risk, such as natural disasters generated by non-human factors, according to the literature on risk society. According to Giddens and Becks (1998), humans are exposed to new hazards in modern society, such as pollution and crime, as a result of the modernisation process. These two sorts of dangers are defined by Giddens (1998) as external risks and artificial risks. As a high-level human agency involved in developing and reducing such hazards, such risks are identified.

The RST involves the general public. As a result of such a society, there has been an upsurge in online connections with people who are not physically present (Olatubosun, 2020). People now have friends from all over the world because to the internet, which has enabled them to form social bonds. The general population is aware of the dangers associated with the changing globalisation atmosphere, such as cyber espionage, identity theft, cyber fraud, and cyber pornography (Harris et al., 2020). According to Beck (1998), there is a curious contradiction in modern society where hazards are increasing rather than decreasing as a result of technical innovation and scientific progress.

The RST entails a tremendous level of risk, one that is so vast that it transcends time and space on a global scale, making risk mitigation seem unachievable. The ultimate risk of cybercrime is that one is oblivious of the dangers that can arise from a single mouse click (Atlam et al., 2020). As the criminal exploits the cover of anonymity to hide effectively, cyber risk prevention would include arming oneself with software and knowledge weapons in a virtual world (Yar, 2019, Gillespie, 2019, Hui, 2017). Technological advancements have resulted in a shift in communication methods, where instead of meeting face-to-face, technology has bridged the gap between people all over the world with just a single mouse click (Maecum, 2019, Lusthaus, 2018, Mbaziira, 2016). Increased vulnerability to human-made dangers has resulted from the risk society and technology advancements.

5.0 THE CYBER SECURITISATION THEORY

The existing literature, on the other hand, defines securitisation as a successful speech act in which an inter-subjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object and to enable a call for immediate and extraordinary measures to deal with the threat (Fouad, 2019, Christou, 2019). Securitisation, according to Waever (1989), entails a referent object that is believed to be threatened, a securitising actor who performs securitisation through a speech act, and an audience that is susceptible to this securitisation. He goes on to say that the securitising Act will be successful if the securitising actor has authority and conducts the speech act according to specific rules. According to Deiber (2012), the CST focuses primarily on the increasing spread of cyberspace controls, and that research shows that governments can control access to information, freedom of speech, and other aspects of cyberspace, despite widespread belief that cyberspace was immune to government regulation in the past.

According to Claessen (2020), securitisation aims to give people the ability to think about security in terms other than military and military activities. According to Nissenbaum (2018) and Lavorgna (2016), the transition from "computer security" to "cybersecurity" required mixing technical discourse with emerging national cybersecurity initiatives, thereby securitizing it. The blurring of the lines between the state and civil society has occurred, according to Saco (2018), because the Internet has challenged established ways of thinking about security and sovereignty. As a result of the CST's distribution of responsibility, private firms are held co-responsible for working with cybersecurity and responding to cyber threats, enhancing the protection of corporations and corporate secrets as well as combating cyber espionage (Hersee, 2019).

The existing literature on CST shows the importance of discussing which unusual measures have been implemented and how well they have been deployed as cyber threats have gotten more secure. The Copenhagen School contends that, given the necessity of security, security discourse should focus on other actors in the debate outside the state or nation. As long as it is working for national or international security and is acknowledged by relevant parties, such a discourse is bringing in other players other than the military to provide security (Hersee, 2019). Many states have seen the birth of a new securitising rhetoric in which persons concerned with digital security identify a wide range of sophisticated cybersecurity challenges by tying computer network security to national security (Stevens, 2016). These concerns span from foreign state digital espionage to terrorists' use of hacking, cyber criminality, and, most importantly, the protection of critical digital infrastructure (Yoon, 2019).

6.0 INTEGRATING RST AND CST

As previously said, existing models or theories for comprehending cyber espionage operate in different ways. According to the RST, internet access carries the possibility of becoming a victim of crime (Olatubosun, 2020). The RST focuses on an individual's daily online routine, which exposes them to hazards that could lead to victimisation (Atlam et al., 2020). The RST is likewise largely tested in the United States, and it focuses solely on victimisation rather than crime prevention (Maecum, 2019, Lusthaus, 2018). The RST is commonly used for a variety of offences, including cyber terrorism, cyber harassment, property crimes, and even cyber theft (Harris et al., 2020). The RST, on the other hand, has been criticised for focusing too much on the risk and neglecting to consider the external risk that comes with it. The RST is also believed to be indifferent to differences in risk concerns within and between countries, regions, or locations. Individualisation and globalisation are argued to be opposed to the logic of industrial modernity, the state, and state-based risk control mechanisms within RST.

The CST, on the other hand, is problematic since it only considers how cyberspace may be built as a security sector (Yoon, 2019). Typically, the CST would apply to areas that need to be secured as a national security danger, such as cyber espionage (Claessen, 2020). The CST is largely tested in western countries like Europe and the United States, and it exclusively concentrates on areas that are considered a national security danger (Hersee, 2019). The CST has been criticised for the high level of formality in the discursive activity of security, saying that this culminates in the idea of security as a speech act with a set, permanent, and unchangeable code of conduct. Furthermore, according to Hart (2018), CST prioritises security over all other concerns and issues, which may jeopardise civil liberties. As a result, a society must understand that in order to achieve security, some freedom must be sacrificed. The research has a gap in that neither RST nor CST have been tested to understand cyber espionage and how to avoid it.

As a result, integration between the two theories is essential because they both complement each other. The RST focuses on the individual's daily activity, which exposes them to hazards that must be managed. However, such criminality cannot be prevented without securitization, and it will pose a threat to national security. The CST focuses on a controller's responsibility in securing an item in order to prevent and better govern such crime or threat (Sperling & Webber, 2019). Predicting the perpetration of crime would be more complete and preventive interventions could be achievable with the linked ideas of the Risk Society and Cyber-Securitisation. The importance of risks and securitization in accounting for not only the perpetration of crime but also lifestyles and normal activities that are associated to the commission of a crime has been recognised in recent victimology research (e.g., Pratt, Turanovic, Fox, & Wright, 2014; Reyns, Henson, & Fisher, 2014; Schreck, 1999; Turanovic & Pratt, 2014). Given the challenges that the existing RST and CST pose on their own, it is necessary to combine the two theories in order to obtain a complete and comprehensive model for preventing cyber espionage.

7.0 CONCLUSION

The current legal landscape on cyber espionage is still very vague internationally as there are no specific laws in place to combat cyber espionage. However, depending on the activities involved in such crime like hacking or modification of data or program, certain cyber law such as the CCA 1997 would apply. Cybercrime may be prosecuted under traditional criminal legislation, such as the Penal Code. In understanding and preventing such crime, it is imperative to adopt the RST and the CST to understand, manage and mitigate the risks of cyber espionage. The RST and CST when applied separately may be deficient in explaining the risks and perpetration of the said crime. Hence, the understanding of such crime by the stakeholders and policymakers could be enhanced by merging both theories. Similar implications may also apply to corporate entities and computer users as the theories aimed at individual responsibility in mitigating the risks of cyber espionage and preventing it. Such move would augur well for the reduction of crimes as envisioned in National Security Policy 2017, the National Security Council Act 2016 and the Sustainable Development Goals No 16 on promoting peace, justice and social institutions.

ACKNOWLEDGMENTS

This work was supported by research grant FRGS/1/2019/SSI10/UITM/02/2 by the Research Management Centre, UiTM Shah Alam, Selangor.

REFERENCES

[1] J. Abd Jalil, H. Hassan, N. Abd Rahman, R. B. R. M. Ali, D. Mohamed, A. Najib, “Business under Threat: The Criminal Liability of Trade Secret Theft in Malaysia?”, International Journal of Business & Society, vol. 21, 2021.

[2] A. Ahmad, “A cyber exercise post-assessment framework: In Malaysia perspectives”, Ph. D dissertation, University of Glasgow, Scotland, 2016.

[3] I.A. Barnes, “Implementation of Active Cyber Defense Measures by Private Entities: The Need for an International Accord to Address Disputes”, Ph. D dissertation, Naval Postgraduate School, Monterey, United States, 2018.

[4] Z, Bederna, T. Szadeczky,” Cyber espionage through Botnets” Security Journal, 1-20, 2019.

[5] J. Caravelli, “The Geopolitics of Cyber and Cyber Espionage”, Cyber Security: Threats and Responses for Government and Business, vol. 43, pp. 2019.

[6] S. Chesterman, “The spy who came in from the Cold War: Intelligence and International Law”’, Michigan Journal of International Law, vol. 27, pp.1071, 2005.

[7] R.J. Deibert, R. Rohozinski, A. Manchanda, N. Villeneuve, G. M. F. Walton, “Tracking ghost net: Investigating a cyber espionage network”,2009.

[8] G. B. Demarest, “Espionage in international law”. Denv. J. Int'l L. & Pol'y, vol. 24, pp. 32, 1995.

[9] M. D.Cavelty, “From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse” International Studies Review, vol. 15(1), pp. 105-122, 2013.

[10] D. P. Fidler, “Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies”, ASIL Insights, vol. 17(10), 2013.

[11] L. P. Hansen, *The Spy Who Never Has to Go Out Into the Cold: Cyber Espionage*, In Encyclopaedia of Criminal Activities and the Deep Web (pp. 258-270). IGI Global, 2020.

[12] D. Herrmann, *Cyber Espionage and Cyber Defence*, In Information Technology for Peace and Security, pp. 83-106, Springer Vieweg, Wiesbaden, 2019.

[13] S. Hore, and K. Raychaudhuri, *Cyber Espionage—An Ethical Analysis*. In Innovations in Computational Intelligence and Computer Vision, pp. 34-40, Springer, Singapore, 2021.

[14] M. Jalali, “Espionage in Modern International Law and Necessity of Codification of Global Provisions”, Public Law Studies Quarterly, vol. 51(1), pp. 329-354, 2021.

[15] S. Khan, N. Khan, & O. Tan, “The efficiency of the legal and regulatory framework in combating cybercrime in Malaysia”, in Understanding Digital Industry: Proceedings of the Conference on Managing Digital Industry, Technology, and Entrepreneurship (CoMDITE 2019), July 10-11, 2019, Bandung, Indonesia (p. 333). Routledge.

[16] K. Kittichaisaree*, Cyber espionage*, In Public International Law of cyberspace, pp. 233-262, Springer, Cham, 2017.

[17] M. C. Libicki, “Drawing inferences from cyber espionage” in 2018 10th International Conference on Cyber Conflict (CyCon), IEEE, pp. 109-122, 2018

[18] M. Longobardo, “Cyber Espionage and International Law, Israel Law Review, vol. 53(2), pp. 294-297. doi:10.1017/S0021223720000011, 2020.

[19] N. L. Nardi, “Origin of Cyber Warfare and How the Espionage Changed: A Historical Overview.”, Transdisciplinary Perspectives on Risk Management and Cyber Intelligence, pp. 145-153, IGI Global, 2021.

[20] G. O'Hara, “Cyber-Espionage: A growing threat to the American economy”, CommLaw Conspectus, vol. 19, pp. 241, 2010.

[21] N. Perlroth, (2019). *Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies*,[Online]. Available at https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html

[22] S. Perumal, S. A. Pitchay, G. N. Samy, B. Shanmugam, P. Magalingam and S. H. Albakri, “The transformative cybersecurity model for Malaysian government agencies”, International Journal of Engineering and Technology (UAE), vol. 7(4.15), pp. 87-92. https://doi.org/10.14419/ijet.v7i4.15.21377, 2018.

[23] D. S. Reveron, *Cyberspace And National Security: Threats, Opportunities, And Power In A Virtual World*, Georgetown University Press, 2012.

[24] A. Rodricks, J. Puri, “Unravelling the translucent theories on espionage: A periodical study on Crime and Security”, Journal of Legal Studies and Criminal Justice, vol.1(1), 2020.

[25] D. Rubenstein, Nation-State Cyber Espionage and its Impacts. Retrieved on October 7, 2017.

[26] C. P. Skinner, "An international law response to economic cyber espionage", Conn. L. Rev., vol. 46, pp. 1165, 2018.

[27] J. G. Spataro, "Iranian Cyber Espionage", Ph. D dissertation, Utica College, United States, 2019.

[28] C. S. Teoh, K. Mahmood, "Is NIST CSF applicable to developing nations? A case study on Government Sector in Malaysia", Pacific Asia Conference on Information Systems (PACIS). Association for Information Systems, 2017.

[29] P. Thomas, L. Hanley "Political warfare in the digital age: cyber subversion, information operations, and 'deep fakes", Australian Journal of International Affairs, vol. 74:4, pp. 439-454, DOI: 10.1080/10357718.2020.1734772, 2020.

[30] G. Wangen, "The role of malware in reported cyber espionage: a review of the impact and mechanism", Information, 6(2), 183-211, 2015.

[31] Yogesh Hole et al 2019 J. Phys.: Conf. Ser. 1362 012121