NEGREI
Academic Journal
of Law and Governance

Institut Agama Islam Negeri (IAIN) Curup, Indonesia
ISSN 2775-8621
volume 1, number 1, 2021
DOI: http://doi.org/10.29240/negrei.v1i1.2570

How does the Goverment Legally Respond to the Cyber Attack? Cases in Australia, People's Republic of China, and India

Edho Aqmal Hakim
Macquarie University, Australia
edho-aqmal.hakim@students.mq.edu.au

Abstract. In the 21st century, cyber attacks are one of the biggest threats to international peace. The aim of this paper are to compare responses of different governments in this case Australia, People's Republic of China and India. Literature study provides a variety of information that is processed by comparative analysis. Three countries have their own approach to answer this cyber attacks issue by founded their own cyber security agencies. In recent years, these countries were able to develop and integrated strong defense mechanism against cyber attacks. While international cooperation and international laws against cyber attacks have not yet to be born, applying multi layered defense of active and passive defenses in their own country is the best option to choose so far. However, each country needs to evaluate the impact of cyber attacks and whether their responses have been effective in dealing with these cyber attacks using quantitative analyzes.

Keywords: Comparative Analysis; Cyber Attacks; Defence Mechanism

Introduction

In the 21st century, cyber attacks are one of the biggest threats to international peace. Unfortunately, international laws have demonstrated to be powerless to prevent cyber attacks since some powerful countries, allow their hackers to work with immunity when their hackers aim rival countries.

Stavola (2016) described cyber attack as an effort to damage or destroy a computer network or system by hackers. Stavola (2016) added, cyber attacks can be divided up into four essential subjects: Viruses, Ransomware, Spyware, and Identity Thieves. Committee on National Security Systems (CNSS) define a cyber attack as: "*An offensive actions over cyberspace, aiming an organization's use of cyberspace intended for disrupting, disabling, destroying, or forcefully controlling a computing infrastructure/ environment in malicious manner; or damaging the integrity of the data or taking restricted information* without permission (Hansche, 2006)".

From those definitions, it is obvious that cyber attack may vary from basic operation of installing virus or spyware on a civilian's personal computer to an attempt to demolish the facility or infrastructure of whole states/ nations. Since the early development of computer and interconnected network, cyber attacks have become progressively dangerous, complex, and sophisticated (Karnouskos, 2011). Compared to previous year, Symantec Internet Security Threat Report (2019) stated that the web attacks and number of attack groups using destructive malware rose 56% and 25%, respectively. Other findings from Data Breach Investigations Report by Verizon in 2019 revealed that 43% of the breach's victims are small business, 16% to public sector entities, 15% to healthcare organizations, and 10% financial industry as shown in figure 1.

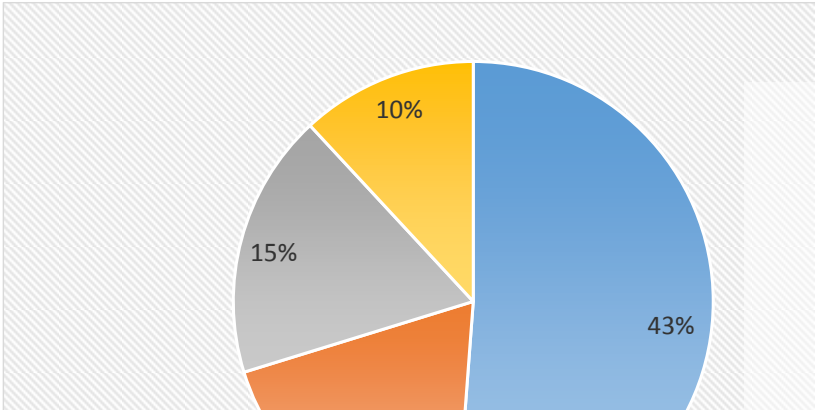

Figure 1. Who are the Breach's Victims? (Verizon, 2019)

Moreover, Verizon (2019) added that throughout the years Organized Criminals and State-Affiliated Operations remain at the top of the cyber attack threat

actors list. This is followed by fluctuated position of System Administrator, Activist and Cashier as shown in figure 2.

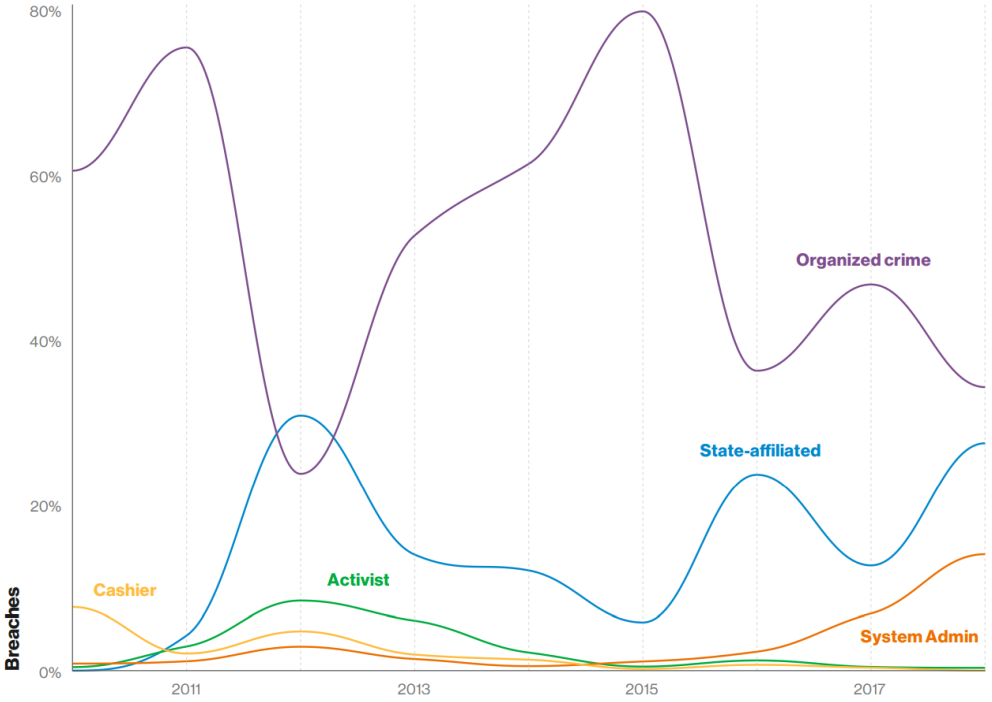

Figure 2. Threat actors in breaches over time (Verizon, 2019)

Ideally, nations and states would cooperate to solve cyber threat, but many major countries refuse to take their international duty seriously because the non-state actors mostly operated behind their back. At the end of the day no country wish another country to use unnecessary force within its boundaries just to deal with cyber attack.

Takahashi and Kadobayashi (2015) illustrated that in a cyber community, malware for example viruses and worms can invade any computing machine outside the boundaries of the nation not only the source but also the target, and an attacker can strike computers all around the globe by deploying another hacker's pre-engineered malicious software. It is implying that a hacker can attack computing systems in state X by commanding computers in state Y while inhabiting physically in state Z. Additionally, with rapid development of hacking technology a system's liability might be vulnerable to attackers across the globe (Takahashi and Kadobayashi, 2015).

As the origin of threats is capable to cross boundaries of nations and states, it becomes clear that cyber attacks potentially can cause devastating consequences. It is important for states to effectively defend their critical infrastructure from cyber attack. According to Carr (2012), the most effective approach to fend off cyber attacks is to apply multi layered defense of active and passive defenses. Unluckily, nation and states consciously decide to restrict their computer defenses solely to passive defenses, in part out of fear that using active defenses violates the law of war (Carr, 2012).

Carr (2012) also explained that complete international treaty to regulate cyber attacks is not exists at the moment. For that reason, nations and states must apply law by analogy: either assimilating cyber attacks to criminal action and responding to them accordingly domestic criminal laws or assimilating cyber attacks to traditional armed attacks and addressing with them accordingly the law of war (Carr, 2012). Moreover, Carr (2012) added the predominant view of nations and academicians is that nations and states should consider cyber attacks as a criminal situation (1) based on doubt if a cyber attack may indicate as an armed attack, and (2) prior answering with force, law of war demands nations and states to describe an armed attack to its agents or a foreign government.

This limited view of the law of war as stated by Carr (2012) are tricky and difficult for two reasons. First and foremost, since active defenses are a shape of digital power, it restricts nation and state computer defenses solely to passive defenses, which lessens nation and state defense stance (Carr, 2012). At a second aspect to respond cyber attacks, nations and states drives to depend on domestic criminal laws, which are not effective since multiple number of powerful nation and states such as China and Russia are reluctant to deport or extradite or prosecute their attackers (Carr, 2012). In these circumstances with the predominant opinion of the law of war, in the middle of cyber attack nations and states end up finds itself in a "response crisis", pushed to take make a decision among more effective, yet it may be argued illegitimate, "active defenses", and the less effective, yet legitimate, "passive defenses" and criminal laws (Carr, 2012).

Despite the fact that nations and states can track down cyber attacks to the origin computer servers in other country, confirming the identity of the hacker needs the support and help from the country of origin with time-consuming and intensive investigation (Carr, 2012). Considering the fact that nonstate threat actors carried out larger part of cyber attacks, there should be no wonder that nations and states are unwilling to address cyber attacks as acts of war and risk breaking international law (Carr, 2012).

However, nations and states who violate the duty to stop cyber attacks and deny to adjust their conducts could be held responsible according to the law of war

for all further attacks from their boundaries (Carr, 2012). Therefore, active defenses can legally use by authority against states that violate their duty to prevent cyber attacks (Carr, 2012). In a moment when cyber attacks become global security threat and country are rushing to discover methods to enhance their cyber defenses, there is no justification to cover sanctuary countries to use active defenses by victim-countries in lawful manner, and any justification to enhance country defenses to cyber attacks by using active defenses (Carr, 2012).

This aim of this paper are to compare responses of different governments in this case Australia, as the country with the highest number of internet users in the Southern Hemisphere (Statista, 2021); also People's Republic of China and India as the top 2 countries with the highest number of internet users in Asia (Miniwatts Marketing Group, 2020). Literature study provides a variety of information that is processed by comparative analysis.

Results and Discussions

Australia

As reported by Davies (2009), Australian government carried out initiatives to establish and provide a new cyber warfare capability under Australian Defense white paper in 2009. Department of Defense of Australia, (2009) stated that development of a Cyber Security Operations Centre to manage and coordinate responses to incidents in cyber world, also the new division shall be composed of greatly-improved capacity to response cyber incident and circumstantial awareness with no particular reference to offensive capability. Nevertheless, Department of Defense of Australia (2009) indicates it will be existed to optimize Australia's strategic range and capability in cyber space.

For achieving that goals, during Australia-United Kingdom Ministerial Consultations in January 2011, Australia praised the prospect to enhance partnership with the United Kingdom on cyber cases and declared they will use their current shared operation on cyber security by further expanding the cooperation of their cyber security divisions and authorities for the groundwork of a sophisticated cyber collaboration. Later in the following months, a new cyber investigations squad started in March 2011 by the Australian Security and Intelligence Organization, tasked with advising and investigating on state-funded cyber attacks engaging Australia (Morden, 2011).

Furthermore, Carr (2012) described strong partnership between the Defense Signals Directorate's Cyber Security Operation Centre and the Australian

Computer Emergency Response Team allow identification and response of threats more efficient and effective. Later in 2014, Australian Cyber Security Center (ACSC) was founded and replacing former Cyber Security Operation Centre. ACSC is the key operational elements of the Australian Government's cyber security capabilities to reduce the security risk to networks, systems and targets of cybercrime (ACSC, 2017).

Recently on 7 April 2020, a department of Australian Government reported to ACSC regarding spoofed COVID-19 themed phishing campaign email to one of senior staff member. Embedded malicious software that designed to steal credential information like banking usernames and passwords was found in email attachment (ACSC, 2020). The ACSC officially submitted a take-down request with the domain registrar located in South Africa and made contact to Australia's main telecommunications companies, as well as Microsoft and Google, to block the access for this website (ACSC, 2020).

People's Republic of China

As stated by Radziszewski et al (2019), in 1997 China began their interest in cyber warfare to compensate their common inferiority compared with Russia and United States, at current time China marking their rivals by using cyber activities. In 2002, the People's Liberation Army has established Information Warfare militia units that incorporate manpower resources from the private sector, universities, and military (Carr, 2012).

Lam (2010) explain according to the Five-Year Plan (2011–2015) by both of the People's Liberation Army and the Chinese central government, the research and development in cyber surveillance is examined as main strategy. Sharma (2011) added Science and Engineering University of People's Liberation Army is exercise center of the IW. The China's Integrated Network Electronic Warfare is the official information warfare strategy that puts network defense and intelligence-collection duties on the specialized information warfare militia units and Signals Intelligence Division of People's Liberation Army 3rd General Staff (Carr, 2012).

As a consequence of Chinese government's enormous actions to enhance cyber warfare capabilities, it is difficult to control and harness increasing squad of cyber experts and hacktivists (Noonan, 2010). Chou (2011) stated, for advocating loyalty and encouraging nationalism within the personnel, Chinese civilians who are assigned for cyber warrior training are first sent to military facilities. A cyber command unit with 30 primary individuals called "Blue Army" squad had created in May 2011, they were employed private sector experts, students from university, officers, and current People's Liberation Army soldiers (Lewis, 2011).

Carr (2012) added that Blue Army squad potentially will work as an arranger and concentrate to the various hacktivists networks in large extend. Actually, the squad's composition differs from the People's Liberation Army information warfare idea, rather than created a military operations command, it utilizes current cyber experts and the hacktivists (Danchev, 2011).

Cyber offensive capabilities of People's Liberation Army and China's government are lightly separated. The People's Liberation Army is more concentrated on cyber warfare capabilities or gathering technology to disarm communication networks of adversary with single strike (Carr, 2012). On the contrary, the China's central government concentrate on resources and hacktivists to suppress or shut down political dissenters and also to increase technological and economic successes over the utilization of cyber surveillance (Hudak et al., 2011). They have utilized organic cyber experts and hacktivists to steal or develop attack code or instruments, in order to acquire this evolving part of cyber capabilities (Krekel, 2009).

Sanger (2018) explain, to guarantee that their internal security agencies knew precisely who was on the Chinese Internet, and what they were talking about, the China's central government enforced stricter requirements every year. Furthermore, Sanger (2012) stated, the authorities obligated that users use their real identity as mandatory, not anonymous, and finally required internet enterprises whose operating Chinese traffic to store all servers physically placed within China. Sanger (2018) added, as the limitations intensified such as censorship requirements, western media companies faced an unavoidable option: obey China's regulations or slowly get kicked out of the world's biggest market. While Bloomberg and others complied and accepted to censor, Google pulled out from mainland China in 2010 (Sanger, 2018). In the following years, in numerous forms, this political agenda would play out time after time, with Apple and Microsoft, Facebook and Uber, one by one have got to make its peace with the China Regulations: give the central government not only access to enterprise's information but also fundamental technology, or get out (Sanger, 2018).

India

According to Thomas (2011), Indian government asked their authorities to reinforce their cyber warfare competencies in August 2010. The strategy instructed government authorities to establish Computer Emergency Response Team for various sectors, enhance abilities to infiltrate adversary nation-states networks, establish an experiment facility, establish hacker laboratories, and

develop countermeasures (Carr, 2012). The lead authorities of this strategy were the Defense Intelligence Agency, the Defense Research and Development Organization, and the National Technical Research Organization (Cybernaut, 2010). In short period of time after the strategy was published, India found out a Chinese version of the Stuxnet worm in Indian critical infrastructure facilities such as communication satellite (Khanna, 2010). Later in December 2010, India's Central Bureau of Investigation website which assumed one of the nation's most secure websites got defaced by Pakistan Cyber Army's hackers (NDTV, 2010). Since then, India has accelerated measures in its offensive cyber abilities (Khanna, 2010).

National Security Council Secretariat of India received report that in 2018 approximately 35% of cyber attacks were originated to China, though disastrous effect in vital facilities and casualties have not caused by those attack (Radziszewski, 2019). Above 55% of cases in between 2010-2018, China's primary objective against India was to have access to classified information from the private sector and the government (Radziszewski, 2019). During the 6th Cyber Security India Summit 2020 in New Delhi, Lieutenant General Rajesh Pant as the National Cyber Security Coordinator said that the Indian government is creating new cyber security policy that could deal all Cyber Ecosystem's issues such as standardization, testing, auditing and capacity development (India Times, 2020).

Comparation

According to Carr (2012), the most proper kind of power to response cyber attacks are "active defenses" in consideration of the principles of *jus in bello* (regulations or conducts of parties engaged in an armed conflict). With regard to military necessity, to complete the task of defending against a cyber attack, active defenses possibly represent all the force required since it can instantly interrupt it by traceback an attack to its origin (hack-back), while traditional weapons not only will be least effective and slower but also potentially break the principle of necessity by utilizing force simply for the interest of destruction's (Carr, 2012).

With regard to proportionality, compared to traditional weapons, active defenses are unlikely to create excessive collateral damage or incidental injury, the traceback abilities enable to target only the origin of a cyber attack and active defenses offer the states a method to surgically strike at their attacker with reasonably reduced risks (Carr, 2012). Moreover, since nonstate actors carried out the majority of cyber attacks, it seems less likely the computers that serve as a state's critical infrastructure will be used as the source to launch the attacks (Carr, 2012). Finally, whereas not holding back from *jus in bello*, picking the active

defenses over the traditional weapons could lower the probability of rising these circumstances toward full-scale armed conflicts between nations and states (Carr, 2012).

Australia, People's Republic of China and India apply the *jus in bello* principle as an offensive strategy in responding to cyber attacks because defensive armed force is still a challenge. Every country is making every effort to form a cyber army in response to cyber attacks carried out by other countries. Nonetheless, India, which in 2020 is still discussing appropriate cybersecurity policies for all sectors, is lagging behind when compared to the People's Republic of China which is developing cyberpower to enhance cyber surveillance. In fact, Australia is collaborating with other developed country to optimize its defense strategy in the face of cyber attacks.

When powerful country refuse to participate in international duty to prevent and fight against cyber attack, victim countries is always find themselves in disadvantage position when most of non-state actors who conduct the cyber attack originated from those powerful country. The most effective approach to fend off cyber attacks is to apply multi layered defense of active and passive defenses.

Conclusion

Australia, People's Republic of China and India have their own approach to answer this cyber attacks issue by founded their own cyber security agencies. In recent years, these countries were able to develop and integrated strong defense mechanism against cyber attacks. While international cooperation and international laws against cyber attack have not yet to be born, applying multi layered defense of active and passive defenses in their own country is the best option to choose so far. However, each country needs to evaluate the impact of cyber attacks and whether their responses have been effective in dealing with these cyber attacks using quantitative analyzes from various approaches, for example risk analysis.

Bibliography

Australian Cyber Security Centre (ACSC), 2017. ACSC threat Report 2017. Australian Government. Available at: https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf (accessed 22 May 2020).

Australian Cyber Security Centre (ACSC), 2020. Threat update: COVID-19 malicious cyber activity. Australian Government. Available at: https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020 (accessed 22 May 2020).

"Australia-United Kingdom Ministerial Consultations," Joint Communiqué, Australian Minister of Foreign Affairs, January 18, 2011, https://webarchive.nationalarchives.gov.uk/20121211162349/http://centralcontent.fco.gov.uk/resources/en/pdf/central-content-pdfs/news/aukmin-iii-joint-communique (accessed 20 May 2020).

Carr, J. *Inside Cyber Warfare, Second Edition*. California: O'Reilly Media, Inc., 2012.

Cybernaut, 2010. "India to increase its cyberwarfare capabilities," The Cybernaut, September 5, 2010, accessed August 30, 2011, http://www.thecybernaut.org/2010/09/india-to-increase-its-cyberwarfare-capabilities/ (accessed 20 May 2020).

Chou, E., 2011. "US-China Cyber War Scenario in the Eyes of a Chinese Student," The Atlantic, February 8, 2011, accessed August 30, 2011, http://www.theatlantic.com/technology/archive/2011/02/us-china-cyber-war-scenario-in-the-eyes-of-a-chinese-student/70855/ (accessed 20 May 2020).

Davies, A. (2015). Intelligence, Information Technology and Cyber Programs. *Security Challenges*, *5*(2), 81-87.

Danchev, D., 2011. "People's Information Warfare Concept," Mind Streams of Information Security Knowledge, entry posted October 5, 2011, accessed August 30, 2011, http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html (accessed 20 May 2020).

Department of Defence, Defending Australia in the Asia-Pacific Century: Force 2030 (Canberra: Commonwealth of Australia, 2009), para. 9.87–88.

Hansche, S. In Official (ISC)2® Guide to the CISSP®-ISSEP® CBK®, *1st Edition*. Florida: CRC Press (Auerbach Publications), 2005.

Hudak, T., Krajkowski, Z., and Salerno, A., 2011. "Chinese Cyber Focus Likely On Enemy Military Networks; During Preconflict, China Likely To Use

Cyber Attacks To Disrupt Enemy Infrastructure Using All Assets," Wikispaces, accessed August 30, 2011, http://chinesehackingdisposition.wikispaces.com/ (accessed 20 May 2020).

India Times, 2020. Government likely to announce new cyber security policy in three months. https://economictimes.indiatimes.com/news/defence/government-likely-to-announce-new-cyber-security-policy-in-three-months/articleshow/74580639.cms (accessed 20 May 2020).

Karnouskos, S. *Stuxnet worm impact on industrial cyber-physical system security*. In 37th annual conference of the IEEE industrial electronics society (IECON 2011) (pp. 4490-4494). Melbourne, AU: IEEE, 2011.

Khanna, S., 2010, "The secret cyber war between India and China accelerates," India Daily, October 10, 2010, accessed August 30, 2011, http://www.indiadaily.com/editorial/21800.asp (accessed 20 May 2020).

Krekel, B., 2009, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrup Grumman, accessed August 30, 2011, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (accessed 20 May 2020).

Lam, W., 2010. "Beijing Bones up its Cyber-Warfare Capacity," The Jamestown Foundation: China Brief 10, no. 3 (February 2010), accessed August 30, 2011, http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=36007 (accessed 20 May 2020).

Lewis, L., 2011. "China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers," The Australian, May 27, 2011, accessed August 30, 2011, http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826 (accessed 20 May 2020).

Miniwatts Marketing Group, 2020. Top 20 Countries with highest number of internet users - 2020 Q1. https://www.internetworldstats.com/top20.htm (accessed 20 May 2020).

Morden, J., 2011. "Australian Govt Reveals New Cyberspooks Unit," FutureGov Asia Pacific, March 14, 2011, accessed August 29, 2011, http://www.futuregov.asia/articles/2011/mar/14/australia-reveals-new-cyberspooks-unit/ (accessed 20 May 2020).

NDTV, 2010. "Hacked by 'Pakistan Cyber Army', CBI website still not restored," NDTV, December 4, 2010, accessed August 30, 2011, http://www.ndtv.com/article/india/hacked-by-pakistan-cyber-army-cbi-website-still-not-restored-70568?cp (accessed 20 May 2020).

Noonan, S., 2010. "China and its Double-edged Cyber-sword," Stratfor, December 9, 2010, accessed August 30, 2011, http://www.stratfor.com/weekly/20101208-china-and-its-double-edged-cyber-sword (accessed 20 May 2020).

Radziszewski, E., Hanson, B., and Khalid S., 2019, https://thediplomat.com/2019/07/indias-response-to-chinas-cyber-attacks/ (accessed 20 May 2020).

Sanger, D., E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown Publishing Group, 2018.

Sharma, D. (2011). China's Cyber Warfare Capability and India's Concerns. *Journal of Defence Studies*, *5*(2), 62-76.

Symantec. 2019. Security Internet Threat Report 2019. Available at: https://www.phishingbox.com/downloads/Symantec-Security-Internet-Threat-Report-ISRT-2019.pdf (accessed 20 May 2020).

Statista, 2021. Number of internet users in the Asia Pacific region as of January 2021, by country *(in millions)*. https://www.statista.com/statistics/265153/number-of-internet-users-in-the-asia-pacific-region (accessed 20 May 2021).

Stavola, E., 2016. When Grown Men Cry: Cyber-attacks and how to prevent them. ImageSource, 18(2), p.24.

Takahashi, T., and Kadobayashi, Y. (2015). Reference Ontology for Cybersecurity Operational Information. *The Computer Journal*, *58*(10), 2297–2312. doi: http://dx.doi.org/10.1093/comjnl/bxu101.

Thomas, K., 2010 "India goes on the offensive in cyber warfare," The Hindu Business Line, August 3, 2011, accessed August 30, 2011, http://www.thehindubusinessline.com/todays-paper/article1000443.ece?ref=archive (accessed 20 May 2020).

Ulsch, M.. *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks*, *1st Edition*. New Jersey: Wiley, 2014.

Verizon, 2019. Data Breach Investigations Report 2019. Available at: https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf (accessed 20 May 2020).