AN ANALYSIS OF THE MEASURES TO COUNTER CYBER ATTACKS

UMMI HANI' BINTI MASO'OD
PROVISIONAL PHD
SCHOOL OF LAW, UNIVERSITY OF LEEDS

ABSTRACT: Cyber attacks have been increasingly acknowledged as a new technological method to wage war. States perceive cyber attacks as a threat to the national security especially the critical national infrastructure. The 2007 incident in Estonia illustrates the severity of the impact of cyber attacks. Estonia's banking, media and government websites were bombarded with Distributed Denial of Service (DDOS) attacks. The attacks crippled the administration and banking system of Estonia for three weeks. Recent years have seen the alarming rise of premeditated cyber attacks with potentially catastrophic effects to the information systems and networks across the globe. The focus of this study is to assess the role of the state and to investigate the measures in countering cyber attacks. This study examines related international and regional instruments, states' practice, domestic legislations, and scholarly writing for the purpose of identifying the measures adopted by states in dealing with cyber attacks. The findings from this study demonstrate that strategies to counter cyber attacks are divided into non-criminal enforcement and criminal liability. Currently, states are focusing on non-criminal enforcement measures such as engaging private entities to strengthen their cyber security. Criminal law have not been fully utilised at this moment in dealing with cyber attacks. This study argues that an integrated approach, which combines non-criminal enforcement and criminal liability, may provide the best solution to counter cyber attacks

KEYWORDS: *Cyber attacks, cyber security, non-criminal enforcement, criminal liability*

1. INTRODUCTION

States have increasingly considered cyber attacks as a serious threat to national security and a challenge to the application of the existing legal norms especially the law of armed conflict.[1] 'The discovery of the stuxnet worm in 2010 was a game-changer in the world of malware'.[2] It is one of the most sophisticated cyber attacks due to its ability to strike from long distance and the specificity of its attack. Iran disclosed that the stuxnet worm had damaged some of its nuclear centrifuges. Estonia also had been subjected to cyber attacks in 2007.[3] The country's banking, media and government websites were bombarded with Distributed Denial of Service (DDOS) attacks. The culprits are suspected to have been the pro-Russian hacktivist.[4] The attacks crippled the administration and banking system of Estonia for three weeks. This event led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence based in Tallinn, Estonia.[5] Georgia was subjected to cyber attacks before the actual usage of conventional

[1] Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013) 3

[2] BBC, 'Researchers Warn of New Stuxnet Worm' (*BBC News Technology*, 19 October 2011) <http://www.bbc.co.uk/news/technology-15367816> accessed 14 January 2014
[3] Schmitt, *Tallinn Manual* (n1) 2

[4] Gallagher M, 'Web War II: What a Future Cyberwar Will Look Like' (*BBC News Magazine*, 30 April 2012) <http://www.bbc.co.uk/news/magazine-17868789> accessed 13 January 2014
[5] Schmitt, *Tallinn Manual* (n1) 1; http://www.ccdcoe.org/

weapons during the 2008 war with Russia.[6] These incidents illustrate the impact of cyber attacks, which can paralyse a country's administration and damage the economy. Computer viruses such as ghosnet can easily penetrate the government's website, tampering with documents and destroying facilities. Furthermore, it has been argued that 'the greater the network integration of a target country's infrastructure, the greater its potential vulnerability'.[7]

Cyber attacks have been increasingly acknowledged as a new technological method to wage war. Alvin and Heidi Toffler examine the notion of the 'Third Wave War'. Due to computerisation, 'Virtually every aspect of warfare is now automated requiring the ability to transmit large quantities of data in many different forms'.[8] They further argue that in the Third Wave War, 'a new breed of knowledge warriors has begun to emerge-intellectuals in and out of uniform dedicated to the idea that knowledge can win, or prevent wars'.[9] The advancement of technology enables states to develop more sophisticated weapons, and this can lead to an arms race in the cyber world. Soldiers are removed further away from the battlefield as 'attacks are carried out through remote-controlled weapons, cyber weapons or robots.'[10] Rid and Mcburney define cyber weapons as 'computer code that is used or designed to be used with the aim of threatening or causing physical functional or mental harm to structures, systems or living being'.[11] ICRC perceives cyber attacks as 'any hostile measures against an enemy designed to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer'.[12] Everyone with a computer connected to the Internet can carry out harmful attacks for various purposes ranging from 'juvenile hacking to organised crime to political activism to strategic warfare'.[13] Thus, similar to conventional weapons, the psychological dimension is pertinent in distinguishing between harmless cyber space activities and cyber attacks. To constitute cyber attacks, the offender must intents to threaten harm or cause harm to the victim and the victim perceives the likelihood of harm being inflicted is real.[14] A new sphere of warfare is created in which attack is done using electronic devises such as desktop targeting other electronic infrastructure. This is different from any ordinary attack using conventional weapons such as missile or tank. The conventional method of warfare requires the presence of soldiers physically to carry out the attack. Cyber attacks on the other hand enable states to attack the military infrastructures of their enemy by using cyber weapons from within the comfort of their own territory. This alleviates the need to deploy soldiers

---

[6] Handler SG, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stan J Int'l L 209

[7] Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1

[8] Toffler A, Toffler H, *War and Anti-War. Survival at the Dawn of the 21st Century* (Warner Books 1993)

[9] ibid 181

[10] 34th Round Table on Current Issue of International Humanitarian Law, San Remo, 8-10 September 2011. Conclusions by Dr Philip Spoerri, Director For International Law and Cooperation, ICRC

[11] Rid T and Mcburney P, 'Cyber-Weapons' (2012) 157 The RUSI Journal, 157:1, 6-13

[12] http://www.icrc.org/eng/resources/ihl-databases/index.jsp

[13] Cavelty MD, Cyber Threats in *The Routledge Handbook of Securities Studies* (Cavelty MD and Mauer V eds, Routledge 2010) 182

[14] ibid

on the battlefield and can minimize casualties. Furthermore, cyber attacks can be perpetrated by anyone who is armed with the necessary equipment and technology. It is difficult to trace the perpetrators, as 'anonymity is the rule rather than the exception'.[15] Corporations, individuals and terrorist groups have the resources to conduct cyber operations.[16] Thus, the likelihood of the proliferation of cyber attacks is higher in comparison to other forms of warfare. Consequently, the phenomenon of cyber attacks raises issues particularly in ascertaining the appropriate means of redress.

2. MEASURES TO COUNTER CYBER ATTACKS

States are faced with an arduous task in regulating activities in the cyber world. This is due to the complex and resilient nature of the Internet, which consists of a myriad of interconnected global network of nodes. The development of the Internet is a double-edged sword, bringing positive and negative effects to the modern world. The Internet has contributed significantly to the growth of the capitalist economy and the society at large. Nevertheless, Internet is a powerful tool that can be used to influence or manipulate its users. Castells further argues that:

> Switches connecting the networks (for example, financial flows taking control of the media empires that influence political processes) are the privileged instruments of power. Thus, the switches are the power holders. Since networks are multiple, the inter operating codes and switches between networks become the fundamental sources in shaping, guiding and misguiding societies'.[17]

Besides cyber attacks, the Internet has been used as a medium to commit illegal activities such as spreading obscene and racist content, theft, fraud, hate speech and online stalking.[18] Thus, managing the Internet has been difficult for the governments especially as their capability is restricted due to the absence of physical territory in the cyber world. This corresponds with the argument that the role of the government in the post-modern world would be limited. According to Beck 'In late modernity at the tail of the century, the traditional state is withering away as a special creature as the structure of a sovereignty and as hierarchical co-ordinator'.[19] The responsibility of the government should be redefined in which certain archaic and dubious tasks need be abolished.

States are moving forward with the privatisation of the criminal justice and security system. This is demonstrated by the increase of private security firms and privatisation of prison. In the postmodern era, the private sector is more involved in policing.[20] The limitation of intervention by states renders an active role by private bodies in managing the Internet. Scholars have examined the concept of governance in postmodern world. Due to the weakening of the notion of statehood, 'one can expect a trend towards governance rather than the government

---

[15] Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2013) 94 International Review of the Red Cross 533

[16] Caytas JD, 'Cyber Warfare as a Superficially Tempting Low-Level Engagement Strategy' <http://ssm.com/abstract=2348842>

[17] Castells M, *The Rise of the Networks Society*, vol 1 (2nd edn, Blackwell Publishing 2000) 75

[18] Akdeniz Y, Walker C, Wall D (eds), *The Internet, Law and Society* (Longman 2000)

[19] Beck U, Giddens A, Lash S, *Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order* (Polity Press 1994)

[20] Akdeniz, *The Internet, Law and Society* (n18) 19

in which the role of the nation state is no longer ascendant'.[21] The governance of the Internet involves 'a wide variety of public and private, state and non-state, national and international, institutions and practices'.[22]

Despite the obstacles faced by states in governing the cyber world, privatisation or contracting the private sector is not the only solution; it requires further consideration. According to Osborne and Gaebler:

> Services can be contracted out or turned over to the private sector. But governance cannot. We can privatise discrete steering functions, but not the overall process of governance. If we did, we would have no mechanism by which to make collective decisions, no way to set the rules of the marketplace, no means to enforce rules of behaviour.[23]

The function of the state is eroding or perhaps 'withering away' due to factors such as globalisation and the rapid growth of supranational planetary organisations.[24] However, the role of the state in maintaining national security, criminal justice, law and order is still intact. Bauman argued that 'To focus locally on the safe environment and everything it may genuinely or putatively entail, is exactly what market forces by now global and so exterritorial want the nation state to do'.[25] Furthermore, the goals of private security providers are different from the values uphold by the criminal justice system. Zedner observes that 'Private security is about satisfying the personal demands of those who pay, ensuring a continuing return upon investments, and keeping shareholders happy. It has little interest in upholding the rule of law, providing authoritative expressions of common values or ensuring social solidarity'.[26]

The aim of governance is to regulate the contents and activities in the Internet. This can be achieved through the engagement between states and private actors. It was reported that the workloads of the police force in developing countries over the past few decades has increased due to the rise of crime rates.[27] Private securities companies are contracted as a supplement to the policing by public police forces especially in conducting surveillance and detective work.[28] As stated previously, Beck argued that the role of the state is primarily to control and design the context of the legal system. Thus, it can be inferred that state is responsible to formulate the policy and the law relating to cyber security. Other fields such as enforcement can be negotiated and delegated to private sectors. Furthermore, working with private security

---

[21] Walker C (ed), *The Criminal Law Review. Special Edition: Crime, Criminal Justice and the Internet* (Sweet & Maxwell 1998)

[22] Ibid 5

[23] Osborne D and Gaebler T, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector* (Addison-Wesley Publishing Company 1992) 45

[24] Bauman Z, *Globalization. The Human Consequences* (Polity Press 1998) 56

[25] ibid 120

[26] Zedner L, *Security* (Routledge 2009) 91

[27] Dijk JV, *The World of Crime. Breaking the Silence on Problems of Security, Justice, and Development Across the World* (Sage Publications 2008) 214

[28] ibid 215

organisations may enhance the maintenance of security and provides administrative and financial reliefs to the states

Reliance on private security firms to manage critical information infrastructures must be done cautiously. The Intelligence and Security Committee of the British Parliament released a report entitled Foreign Involvement in the Critical National Infrastructure: The Implications for National Security in 2013.[29] The report indicated that Huawei, a Chinese telecommunications company was awarded with a contract in 2005 to supply some of the transmission and access equipment including routers across the network from January 2007. The Committee has expressed its concern on the 'potential conflict between the commercial imperative and national security, as a result of increasing private ownership of critical national infrastructure combined with the globalisation of the telecommunications marketplace'.[30] Huawei is perceived to be influenced by the Chinese Government. This cause grave concerns as China is suspected to sponsor attacks for the purpose of gathering information and espionage. Despite of its vehement denial, Huawei has been considered as a security risk by politicians in US and Australia. The Committee suggested the British Government to establish a procedure to assess the risk and to clarify accountability in managing contracts involving critical national infrastructure and foreign investment. Thus, selecting a reliable and trustworthy contractor is utmost important to preserve national security. Profiling is perhaps a necessary measure to ensure the reliability of the firm contracted to guard the critical national infrastructure and enhance cyber security.

The danger of cyber attacks requires responses at the international and domestic level. However, any measures taken against the perpetrators must be real and meaningful. Responses to cyber attacks are not confined to the cyber domain. It may include other areas such as economic, judicial or military.[31] The strategies to counter cyber attacks are divided into non-criminal enforcement and criminal liability. The objective of the enforcement measures is 'to re-establish legality' by ensuring compliance with the legislation, either by preventing or by repressing certain behavior.[32] Enforcement officials can choose between criminal prosecution and civil sanctions or other non-criminal remedies. Their decision depends on various factors such as 'harm, blameworthiness, deterrent effects, alternative remedies or policy options, and resource constraints'.[33]

2.1 NON-CRIMINAL ENFORCEMENT MEASURES

Non-criminal enforcement measures are divided into international, regional and domestic levels. At the international level, cooperation between states in dealing with cyber attacks is essential. Ahead of the London Conference on Cyberspace in 2011, Britain's Foreign Secretary William

---

[29] Foreign Involvement In the Critical National Infrastructure: The Implications for National Security (*Intelligence and Security Committee*, 2013) <http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205680/ISC> accessed 10 July 2014

[30] ibid

[31] House of Commons Defence Committee, *Defence and Cyber-Security. Sixth Report of Session 2012-2013* (2012)

[32] Study On Measures Other Than Criminal Ones in Cases Where Environmental Community Law Has Not Been Respected in the EU Member States' (*Milieu Ltd. and Huglo Lepage Associates*, 2004) <http://ec.europa.eu/environment/legal/crime/pdf/ms_summary_report.pdf> accessed 12 March 2014

[33] Brown DK, 'Criminal Law Theory and Criminal Justice Practice' (2012) 49 Am Crim L Rev 73

Hague stated that 'the internet was revolutionising people's lives but required a global co-ordinated response to ensure its transformative power was fully exploited and channelled in the right direction'.[34] Despite of limited resources and power, international organisations can enhance the global cyber security strategies by promoting the creation of appropriate structures and norms to prevent the malicious use of cyber technologies.[35] Organisations such as United Nations and International Telecommunications Union (ITU) have undertaken measures to address cyber attacks. United Nations has adopted several resolutions relating to the ICTs and cyber security. Resolution A/RES/57/239 of 2003 acknowledges the importance of international cooperation for achieving cyber security through the support of national efforts and calls member states to develop a culture of cyber security in using the information technologies.[36] Resolution A/58/481 of 2004 recognises the vulnerability of the critical national infrastructure due to variety of threats to information network. However, any efforts to protect critical national infrastructure must be done with due regard to the national laws that protect privacy and other relevant legislation. This resolution reiterates the significant of international cooperation in securing critical information infrastructures by coordinating emergency warning systems and sharing of information.[37] Resolution A/65/405 of 2010 acknowledges the adverse effects of technologies in which it can be used for the purposes inconsistent with the objectives of maintaining peace and security and detrimental to the states in both civil and military fields. In this resolution, member states of the United Nations express their concern about the usage of information technologies by criminal and terrorist.[38] A group of experts has been given the mandate to investigate the potential threats in the realm of information security and the measures to address them. Besides that, ITU has founded the High-Level Expert Group on Cybersecurity in 2007 to provide consultation for information security experts from various fields and regions.[39]

Despite of the efforts initiated by the United Nations, resolutions adopted by the General Assembly are not binding on member states. The resolutions recommended actions to be taken by the member states in enhancing cyber security. The United Nations should adopt a firmed stand against states that use the information technology for unlawful purposes such as attacking the critical information infrastructure of another states to disrupt their financial and banking system. In addition, measures undertaken by the United Nations in dealing with cyber security are fragmented and decentralised. Cyber security is dealt separately by the specialised agencies of the United Nations according to their area of expertise. Multilateral treaties played an important role in addressing common problems of states. ICTs and networking technologies

---

[34] Stamp G, 'UK Seeks 'Consensus' at Cyberspace Conference' (*BBC News Politics*, 18 October 2011) <http://www.bbc.co.uk/news/uk-politics-15355739> accessed 14 January 2014

[35] The Cyber Index. International Security Trends and Realities, (*United Nations Institute for Disarmament Research*, 2013) <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> accessed 10 July 2014

[36] Resolution 57/239 Creation of a Global Culture of Cybersecurity, <http://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_Resolution_57_239> accessed 10 July 2014

[37] Resolution 58/199 Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, <http://www.itu.int/int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199> accessed 10 July 2014

[38] Resolution 65/41 Developments in the Field of Information and Telecommunications in the Context of International Security, <http://www.un.org/en/ga/search/view_doc.asp?symbol+AA/Res?65/41> accessed 10 July 2014

[39] The Cyber Index (n35)

are cross-dimensional issues, which affect many societies in several aspects including legal, political, and cultural.[40] It has been suggested that the Security Council can play an active role in providing the legal framework to regulate cyber warfare.[41] Instruments similar to nuclear and biological arms control might be adopted to regulate cyber attacks. However, international legal system does not possess the ability to legislate universal norms due to the principle of state's sovereignty. Only a handful of states favour a world government that would dictate uniform behaviour for all.[42] In addition, the diversity of criminal justice systems throughout the world may hamper the attempt to conclude agreement between states. According to Mcquade, 'International agreements about managing crime are usually very difficult to establish because nations often have very different views as to what constitutes justice'.[43] Consensus has not been reached on key issues such as can certain types of information be considered as weapon and the application of the international humanitarian law to the cyber space.[44]

The role of the regional organisations is pivotal in tackling cyber attacks. The primary aims of the establishment of regional organization are to maintain peace and 'resolving or containing conflicts to avoid further escalation'. [45] The Association of South East Asian Nations (ASEAN) can facilitate cooperation between its member states in countering cyber attacks. National security is an utmost concern among the member states of ASEAN. Article 2 (b) of the 2008 ASEAN Charter provides that member states shared the commitment and are collectively responsible for 'enhancing regional peace, security and prosperity'.[46] The focus of ASEAN is on the development of instruments to address transnational crimes in the region which 'include eight priority areas, namely terrorism, illicit drug trafficking, trafficking in persons, arms smuggling, sea piracy, money laundering, international economic crime and cybercrime'.[47] The ASEAN ICT Masterplan 2015 (ICT Masterplan) was established in order to foster cooperation between the member states of ASEAN in developing the region's ICT landscape.[48] The aim of the ICT Masterplan is to provide affordable ICT access especially to the rural population of ASEAN as part of the project to establish a single ASEAN Community. The ASEAN Telecommunications and IT Minister (TELMIN) leads the effort to realise the objectives of the ICT Masterplan. Among the objectives of the ICT Masterplan is to promote network integrity, information security and data protection. Common standards and framework for information security among member states

[40] ibid

[41] Friesen TL, 'Resolving Tomorrow's Conflicts Today: How New Developments Within The U.N. Security Council Can Be Used To Combat Cvberwarfare' (2009) 58 Naval L Rev 89

[42] Charney JI, 'Universal International Law' (1993) 87 A.J.I.L 529

[43] Mcquade SC, *Understanding and Managing Cybercrime* (Pearson 2006) 282

[44] The Cyber Index (n35)

[45] Caballero-Anthony M, *Regional Security in Southeast Asia. Beyond the ASEAN Way* (The Institute of Southeast Asian Studies 2005) 15

[46] http://www.asean.org/archive/publications/ASEAN-Charter.pdf

[47]ASEAN, 'ASEAN Security Outlook' (*ASEAN*, 2013) <http://www.asean.org/images/2013/resources/publication/asean%20security%20outlook%202013.pdf> accessed 16 February 2014

[48]http://www.asean.org/images/2012/publications/ASEAN%20ICT%20Masterplan%20(AIM2015).pdf

will be developed. Besides that, ASEAN Network Security Council Action will be established to promote CERT cooperation and sharing of expertise.

So far, there is no definite cyber defence policy adopted by ASEAN. The proposed establishment of the ASEAN Network Security Council Action is not sufficient in protecting the regional's critical infrastructures and information system from cyber attacks. It is difficult to establish a binding regulation at the regional level as the decision making process by ASEAN is based on consensus. Thus, any measures to counter cyber attacks will be in the form of directives and guidelines. Member states have the leeway to adopt the directives according to their own needs.

At the domestic level, cyber attacks can be curtailed through various means. Firstly, states may adopt a comprehensive defence strategy. This includes strengthening surveillance capability through the establishment of a national cyber security institution. The advancement of technology allows states to develop programmes to filter or to counter cyber attacks. The defence strategy may also involve battlefield or military responses.[49] It has been suggested, 'a state may use military response to counter malicious cyber operations that fail to qualify as armed attacks'.[50] Countermeasure is a self-help remedy provided under international law. A state may resort to countermeasure upon the fulfillment of certain conditions under international law such as the principle of proportionality.[51] However, the development of a sound defence strategy requires a huge amount of money. Only advanced countries such as UK and US are capable of doing so.

Secondly, the national parliament can pass legislation to tighten the security of the cyber space by monitoring the Internet service providers and related companies. They could have the obligation to ensure a secure cyber system in order to protect the interest of the public. This duty could be extended to assist authorities in its investigation to unravel the identity of the culprits behind cyber attacks. The legislator may create an administrative body to enforce these obligations. This body can be conferred with the powers to inspect and provide remedial action.[52] It can quickly identify the infringing act and provide immediate response to stop further violation. However, issues may arise pertaining to the appropriate sanctions that should be imposed by the administrative body. The legislator may decide to seek redress in the form of monetary compensation or to impose the order for closure or naming and shaming to prevent the commission of cyber attacks.

Besides that, the government may impose regulatory measures such as licensing for all computers, compulsory installation of security software, password and encryption. Computer manufacturers could be compelled to install security software before they are permitted to sell their products. Software companies such, as Microsoft are capable of providing protection to software and encrypting emails. The government may monitor the production of the switches system by companies such as Cisco. Brenner refers the manufacturers of cyber related devices as the 'architects'.[53] She suggested that civil liability and criminal liability should be imposed on

---

[49] House of Commons Defence Committee, *Defence and Cyber-Security* (n31)

[50] Schmitt MN, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' [2014] Virginia Journal of International Law 54

[51] Article 49-53 of the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts

[52] Lepage, Study On Measures Other Than Criminal Ones (n32) 21

[53] Brenner SW, Cybercrime: Rethinking crime control strategies in *Crime Online* (Jewkes Y ed, Willan Publishing 2007) 24

'architects' such as the software industry due to their role in creating and sustaining cyberspace. Software has become essential in the national infrastructures; thus, a system must be devised to ensure that software manufacturers are taking adequate measures to ensure the reliability of their products.[54] Apart from that, as stated earlier, based on the report issued by Intelligence and Security Committee for the British Parliament, regulatory measures can be imposed against local and foreign companies to monitor their activity in managing critical national information infrastructure.

Thirdly, victims may consider the initiation of civil action against the perpetrators of cyber attacks as an alternative to criminal proceedings. The objective of civil liability is to protect private interest by obtaining compensation for the damages or injuries suffered by the victim. In comparison, 'criminal and administrative law seeks to protect public interests'.[55] However, the victims must be able to identify the appropriate cause of action in order to commence civil proceeding. The failure to invoke the right cause of action may lead to the dismissal of the case by the court. The cause of action may be in the form of torts or breach of statutory duty. Besides that, the victims must ensure that they have suffered damages due to the cyber attacks. The victims also may apply for specific relief such as injunction against the perpetrators.

The banking and financial institutions are targets for cyber attacks. Thus, civil action is a viable recourse to seek compensation and to re-establish their reputation. States also can initiate civil action to seek compensation for the destruction of any infrastructure caused by cyber attacks. However, the jurisdiction of the national court is limited with respect to the action initiated against a state and its organs. In *Jones v Saudi Arabia*, the House of Lords decides that Saudi Arabia and its agents are entitled to immunity in civil proceedings.[56] This principle is also affirmed by the ICJ in the case of *Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening)*.[57] In this case, the ICJ suggests that the principle of jurisdictional immunity does not affect the rights of individuals to seek other forms of redress besides the initiation of civil action. State may initiate action on behalf of citizens against another state, which is involved in the commission of cyber attacks on the basis of diplomatic protection. Action also can be taken on the international plane by invoking the principle of state responsibility.

Lastly, the rise of cyber attacks has led to the establishment of security management firms and contractors offering solutions, services and consultation on cyber security. States have relied on these firms to strengthen their defence against future cyber attacks. Private entities have been substantially involved in suppressing and countering cyber attacks. For instance, Internet companies such as Google provides information on cyber security to its users.[58] Computer Emergency Response Team (CERT) Coordination Centre US was established in 1988 in response to the Morris Worm incident. This organisation works together with the government, law enforcement and the academia such as the Carnegie Mellon University to develop advanced methods and technologies to counter cyber threats.[59] Pursuant to the National Cyber Security

[54] ibid 25

[55] Lepage, Study On Measures Other Than Criminal Ones (n32) 9

[56] *Jones (Respondent) v. Ministry of Interior Al-Mamlaka Al-Arabiya AS Saudiya (the Kingdom of Saudi Arabia) (Appellants) [2006] UKHL 26*

[57] ICJ Report 2012

[58] (http://googleblog.blogspot.co.uk/2009/11/next-steps-in-cyber-security-awareness.html)

[59] http://www.cert.org/about/

Strategy 2011, UK government had established the UK National Computer Emergency Response Team (CERT-UK) on 31.03.2014. CERT-UK works together with the industry, government and academia to enhance UK cyber reliance.[60] This agency is responsible to manage the national cyber security incident, to provide support to companies in handling cyber security incidents and to promote cyber security awareness.

In Malaysia, the Ministry of Science, Technology and Innovation established the national cyber security specialist agency, which is known as Cybersecurity Malaysia. [61] This agency is given the task to prevent and minimise disruptions to critical information infrastructure.[62] It provides services such as the management of security quality and research. Besides that, the Malaysia Computer Emergency Response Team (MyCERT) was formed on 13.01.1997 and started its full operation on 1.03.1997.[63] The aims of MyCERT are to reduce attacks and to minimise any consequential damage. MYCERT handles cyber security related incidents such as intrusion, identity theft, malware infection and cyber harassment.[64]

The rise of cyber attacks has led to the establishment of security management firms and contractors offering solutions, services and consultation on cyber security. States have relied on these firms to strengthen their defence against future cyber attacks. For instance, it was reported that UK government has engaged Cassidian, a company specialised in global security solutions and system to monitor its cyber security. Cassidian has three Cyber Defence Centre based in Paris, Newport and Munich, which provide services such as cyber intelligence, crisis management assistance, incidents detection and maintenance of systems.[65] Besides that, Cassidian offers professional training courses on security solutions, cyber security awareness and reaction.[66]

2.2 CRIMINAL LIABILITY

Non-criminal action is appealing to states due to several reasons. Some scholars argue that, 'the resort to the criminal process can be slow, costly and the outcome may be unpredictable. The criminal justice system is an imperfect instrument of social control'. [67] Besides that 'the administrative infringement procedure is normally agreed to be less costly and faster than criminal procedure'.[68] Furthermore, establishing criminal culpability of cyber attacks is difficult. The process of securing a conviction is complicated. This includes identifying the criminals who

[60] Ibid

[61]http://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html

[62] ibid

[63] http://www.mycert.org.my/en/about/about_us/main/detail/344/index.html

[64] ibid

[65] http://www.cassidian.com/en_GB/web/guest/mission

[66] http://www.cassidian.com/en_GB/web/guest/cybersecurity/cybersecurity-training-centre

[67] Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

[68] Lepage, Study On Measures Other Than Criminal Ones (n32) 60

most probably commit the offence in the territory of another state and the process of apprehending the criminals, which may only be done through extradition or mutual legal assistance.

Despite this, criminal law is still needed to regulate activities performed by individuals, which caused harm to others.[69] 'Law is the means by which a community seeks to organise itself and give effect to the basic norms, which it regards as most important'.[70] Beetham argues that the justifiability of the law is evinced from the public sphere. People obey the law regardless of its content due to the legitimacy given to the authority.[71] 'Obedience is therefore to be explained by a complex of reasons, moral as well as prudential, normative as well as self-interested, that legitimate power provides for those who are subject to it'.[72] Heavy reliance on private entities arguably is not sufficient to deal with cyber attacks. According to Fafinski, 'Even though an ideal CERT network seems well suited as a extra-legal response to the problem of computer misuse, it must be recognised that CERTs cannot exist in a legal vacuum. The law still has the role of governing and informing the internal framework within which the CERT operates'.[73] The private entities are not capable of enforcing the law against the people who posed serious threat to cyber security. They can merely assist in the investigation and production of evidence. Thus, they may lack the political will and the power to investigate trans boundary attacks which requires the assistance of the enforcement authorities of the state in which the attacks originated. The intervention by the government is still needed especially in imposing liability and punishing the perpetrators. Legislation and prosecution are necessary to incarcerate computer experts who caused destruction to the national infrastructure and severely obstructing the Internet service. It can be argued that criminal liability is an important reactive measure to counter cyber attacks. 'The criminal justice system is costly to operate, but in exchange offers a mean of controlling harmful activities that, if unchecked, would result in very high costs for victims and the wider community'.[74] Sir David Omand, opined that the likelihood of attack can be reduced by 'catching and prosecuting lower level hacktivists and criminals, and making their activities harder'.[75] Cyber attacks on financial and banking institutions can cause harmful effect to the economy of a state. Thus, criminalising cyber attacks may help to regulate hazardous cyber operations.

One of the most important features of criminal justice is the sentencing of offender. 'Punishment depends for its effect on the response of the individual and the audience, otherwise, as von

---

[69] Mill JS, *Utilitarianism and the 1868 Speech on Capital Punishment* (Sher G ed, 2nd edn, Hackett Publishing Company 2001)

[70] Singh R, 'Law As a System of Values' (2013) <http://www.judiciary.gov.uk/Resources/JCO/Documents/Speeches/singh-law-as-system-of-values20131031.pdf> accessed 14 April 2014

[71] Beetham D, *The Legitimation of Power. Issues in Political Theory* (Jones P and Weale A eds, Macmillan 1991) 13-26

[72] Ibid 27

[73] Fafinski SF, 'Computer Use and Misuse: the Constellation of Control' (PhD, The University of Leeds 2008)

[74] Bowles R, Faure M, Garoupa N, 'The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications' (2008) 35 JL & Soc'y 389

[75] 'Cyber-security: Problems Outpace Solutions' (*Security & Defence Agenda*, 2013) <www.securitydefenceagenda.org> accessed 13 March 2014

Hirsch has observed, being sent to prison would be no worse than joining the crew of a submarine'.[76] Tough responses are essential for those who attack institutions of national importance. 'The institution of punishment gives genuine bindingness to the rule of law by providing significant incentives not to violate legal rules'.[77] Furthermore, criminal liability creates more stigmas, as the process is more public in comparison to the civil law. Arguably, it can deliver credible deterrence and carries public confidence.[78] 'The concept of deterrence is fundamentally premised on the notion that the infliction of a punitive sanction is capable of influencing the future conduct of potential lawbreakers'.[79]

Criminal law may have not been fully utilised at this moment in dealing with cyber attacks. This maybe due to the absence of any recorded cases on the prosecution of cyber attacks and the uncertainty of the mechanisms in dealing with cyber attacks under international law and domestic criminal law. Cyber attacks must be classified as specific crimes under international law to enable the International Criminal Court or other international criminal tribunals to exercise their jurisdiction. 'The principle of Nullum Crimen Nulla Poene Sine lege or the principle of legality in international criminal law provides that at the time the crime was committed, a written or unwritten norm must have existed upon which to base criminality under international law'.[80] Under the domestic law, a criminal act is one defined as such by the penal code or the statutes. It is an act prohibited, prosecuted, and punished by criminal law. Thus, further investigation is needed on the current legislations in Malaysia related to cyber operations in particular the Computer Crimes Act and the proposed Cyber Crimes Act. With more attacks being reported and the increasing gravity of the attacks, companies especially the Internet service provider such as Google may benefits from the intervention by the government in the form of criminal law.

2.3 COMBINED STRATEGIES FOR COUNTERING CYBER ATTACKS

Relying solely on criminal enforcement may not be the most effective approach to counter cyber attacks. 'To adopt punishment as a strategy of first choice is unaffordable, unworkable and counterproductive in undermining the good will of those with a commitment to compliance'.[81] On the whole, an integrated approach, which combines non-criminal enforcement and criminal liability, may provide the best solution to counter cyber attacks. Ian Ayres and John Braithwaite formulated the 'Pyramid of Strategies of Responsive Regulation', which prescribe the phase of enforcement actions for occupational health and safety, environment or nursing home regulation. At the base of the pyramid is persuasion. If the wrongful acts persist, the next layer provides for a warning letter. 'If this fails to secure compliance, imposition of civil monetary penalties; if this fails, criminal prosecution; if this fails, a plant

[76] Smith DJ, 'Less Crime Without More Punishment' [1999] Edinburgh Law Review

[77] Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

[78] Bowles R, The Scope of Criminal Law (n72)

[79] Bishop P, 'Criminal Law as a Preventative Tool of Environmental Regulation: Compliance Versus Deterrence' (2009) 60 N Ir Legal Q 279

[80] Werle G, *Principles of International Criminal Law*, vol T.M.C. Asser Press (2nd edn, 2005)

[81] Ayres I, Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

shutdown or temporary suspension of license to operate; if this fails, permanent revocation of license'.[82] The focus of the pyramid is in its form rather than the content. This is because different sanctions apply to different regulatory arenas.[83] Thus, the same structure with modification is applicable to the enforcement measures in dealing with cyber attacks as indicated in figure 1. At the base of the pyramid are preventive measures such as establishing a sound cyber defence strategies. The next layer is non-criminal enforcement such as civil action, which may take precedence over criminal liability and should be exhausted first. Subsequent to civil action is the imposition of regulatory measures on individuals and corporate entities. At the top of the pyramid is criminal liability, which may be reserved for more sinister and grave offences.

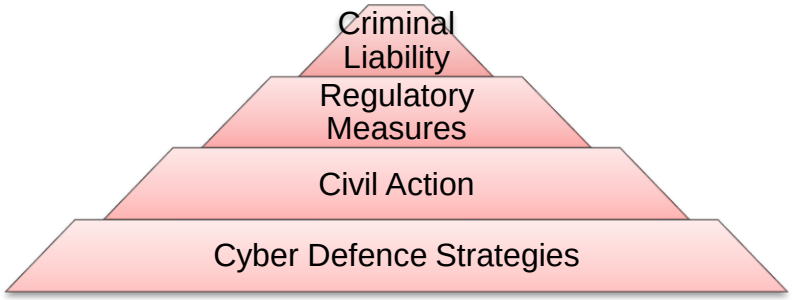

Figure 1: Pyramid of enforcement strategies for cyber attacks

3. CONCLUSION

Cyber attack is an unavoidable problem that must be addressed properly by states. In recent years, states have increasingly engaged private sector for defences, protection, logistics, intelligence, consultancy and security. This inclination is due to the decentralisation of the public sector management in which more core functions of the government have been delegated to new agencies. For that reason, states rely heavily on private security firms in developing the mechanism and strategy to counter cyber attacks in the form of non- criminal enforcement actions. However, with more attacks being reported, intervention by the government in the form of criminal sanction can be used as a symbolic act and deterrence for future attacks.

[82] ibid 35-36

[83] ibid 36

REFERENCES

Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013)
--'"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' [2014] Virginia Journal of International Law 54

Handler SG, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stan J Int'l L 209

Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1

Toffler A, Toffler H, *War and Anti-War. Survival at the Dawn of the 21st Century* (Warner Books 1993)

Rid T and Mcburney P, 'Cyber-Weapons' (2012) 157 The RUSI Journal, 157:1, 6-13

Cavelty MD, Cyber Threats in *The Routledge Handbook of Securities Studies* (Cavelty MD and Mauer V eds, Routledge 2010)

Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2013) 94 International Review of the Red Cross 533

Castells M, *The Rise of the Networks Society*, vol 1 (2nd edn, Blackwell Publishing 2000)

Akdeniz Y, Walker C, Wall D (eds), *The Internet, Law and Society* (Longman 2000)

Beck U, Giddens A, Lash S, *Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order* (Polity Press 1994)

Walker C (ed), *The Criminal Law Review. Special Edition: Crime, Criminal Justice and the Internet* (Sweet & Maxwell 1998)

Osborne D and Gaebler T, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector* (Addison-Wesley Publishing Company 1992)

Bauman Z, *Globalization. The Human Consequences* (Polity Press 1998)

Zedner L, *Security* (Routledge 2009)

Dijk JV, *The World of Crime. Breaking the Silence on Problems of Security, Justice, and Development Across the World* (Sage Publications 2008)

Study On Measures Other Than Criminal Ones in Cases Where Environmental Community Law Has Not Been Respected in the EU Member States' (*Milieu Ltd. and Huglo Lepage Associates*, 2004) <http://ec.europa.eu/environment/legal/crime/pdf/ms_summary_report.pdf> accessed 12 March 2014

Brown DK, 'Criminal Law Theory and Criminal Justice Practice' (2012) 49 Am Crim L Rev 73

Friesen TL, 'Resolving Tomorrow's Conflicts Today: How New Developments Within The U.N. Security Council Can Be Used To Combat Cvberwarfare' (2009) 58 Naval L Rev 89

Charney JI, 'Universal International Law' (1993) 87 A.J.I.L 529

Mcquade SC, *Understanding and Managing Cybercrime* (Pearson 2006)

Caballero-Anthony M, *Regional Security in Southeast Asia. Beyond the ASEAN Way* (The Institute of Southeast Asian Studies 2005)

Brenner SW, Cybercrime: Rethinking crime control strategies in *Crime Online* (Jewkes Y ed, Willan Publishing 2007)

Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

Mill JS, *Utilitarianism and the 1868 Speech on Capital Punishment* (Sher G ed, 2nd edn, Hackett Publishing Company 2001)

Beetham D, *The Legitimation of Power. Issues in Political Theory* (Jones P and Weale A eds, Macmillan 1991)

Fafinski SF, 'Computer Use and Misuse: the Constellation of Control' (PhD, The University of Leeds 2008)

Bowles R, Faure M, Garoupa N, 'The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications' (2008) 35 JL & Soc'y 389

'Cyber-security: Problems Outpace Solutions' (*Security & Defence Agenda*, 2013) <www.securitydefenceagenda.org> accessed 13 March 2014

Smith DJ, 'Less Crime Without More Punishment' [1999] Edinburgh Law Review

Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

Bishop P, 'Criminal Law as a Preventative Tool of Environmental Regulation: Compliance Versus Deterrence' (2009) 60 N Ir Legal Q 279

Werle G, *Principles of International Criminal Law*, vol T.M.C. Asser Press (2nd edn, 2005)

Ayres I, Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

AUTHOR'S BIOGRAPHY

Ummi Hani' Binti Maso'd is currently pursuing her Phd in criminal law. She can be contacted via email lwuhm@leeds.ac.uk.