International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 226-231
The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)

# Data Leak, Critical Information Infrastructure and the Legal Options: What does Wikileaks teach us?

Ida Madieha Abdul Ghani Azmi
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University
Selangor, Malaysia
imadieha@iium.edu.my

Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University
Selangor, Malaysia
sonny@iium.edu.my

Sigit Puspito Wigati Jarot
Kulliyyah of Engineering
International Islamic University
Selangor, Malaysia
sigit@iium.edu.my

*Abstract*—**The massive data leaks by Wikileaks suggest how fragile a national security is from the perspective of information system and network sustainability. What Wikileaks have done and achieved raises some causes of concern. How do we view such leaks? Are they an act of whistle-blowing or disclosure of government misconduct in the interest of the public? Are they the champion of free press? Or are they a form of data breach or information security attack? What if it involves the critical information infrastructure (CII)? Could they be classified as 'cyber-terrorist'? The objective this paper is to outline the problems and challenges that Malaysia should anticipate and address in maintaining its national CII. The paper first looks at Wikileaks as it is the 'icon' of data leaks. Then it examines the causes of data breach before proceeding to foray into the concept of 'critical information infrastructure' in the US and Malaysia. Finally, the paper explores legal options that Malaysia can adopt in preparing herself to possible data breaches onslaught. It is the contention of the paper that the existing traditional legal framework should be reformed in line with the advances of the information and communications technologies, especially in light of the onslaught of data leaks by the new media typically represented by Wikileaks.**

***Keywords-data breach; critical information infrastructure; law and regulation; Malaysia***

## I. Enter the New World of Spider Web

"Wikileaks", an international non-profit organization that runs the online whistle-blower services at the now-defunct website <www.wikileaks.org>, is hailed by the Time magazine as 'the whistle-blower of the digital age'. Its Australian founder, Mr. Julian Assange, was made a candidate for the Time's Person of the Year 2010 award. This prominence was credited to their activities, most notably in the second half of 2010, in disseminating on the Internet hundreds of thousands of secret or confidential documents involving various governments and giant corporations [1].

Among the critical data leaked was the disclosure of a long list of commercial and other installations deemed critical to America's national security. Included in the list are the landing points of undersea cables and the names of firms making vital vaccines. There was also disclosure about NATO's new plans for defending Poland and the Baltic states, which includes disclosure of the code name related to the plans. As it is earlier mentioned, the 250,000 data leaked by the Wikileaks had implicated many countries including Malaysia.[1]

Despite leaking top-classified information such as military and diplomatic communication data, there seems to be uncertainty as to whether or not Wikileaks will finally face any legal actions. It was reported by *The New York Times*, on 7th December 2010 that the US Justice Department was exploring possible charges against WikiLeaks and Assange on the release of diplomatic messages under the Espionage Act 1917 or even on conspiracy or trafficking in stolen property. Meanwhile, Julian Assange had contested in the UK court against his extradition to Sweden over alleged sexual offences, as reported by *The Guardian* on 13th July 2011. Needless to say, Assange and his Wikileaks has gained huge support from all over the world. The incident demonstrates some causes of concern: firstly, a highly critical infrastructure such as that houses the military system and diplomatic cables, despite its sensitivity, are not spared from security breach or intrusion. Secondly, such leak can in turn cause far-reaching damage to public interests, national security and economic interests. Last but not least, the problems cannot be surmounted easily; the hands of law seem incapable of resolving the problem. It does not help that incidence of ordinary data breach is so common that there does not seem to be full proof method to totally eliminate it.

## II. Causes and Trends of Data Breach

Statistics tell us that in the cyber environment, data breaches are everyday phenomena. In a study conducted by Symantec and the Ponemon Institute in their 2011 Cost of a Data Breach Reports, it is found that around half of the causes of data breach can be categorised into system glitch, negligence and malicious attack. Though negligence counts slightly more than malicious attacks, the costs caused by the latter is the highest of all. The reports also revealed that such malicious attacks involve the use of malicious software (viruses,

[1] See, for examples, "WikiLeaks: Malaysia didn't inform US of missing jet engines," *The Malaysian Insider*, 15th February 2011; "WikiLeaks: Malaysia loses game of "chicken' with Singapore over bridge," *The Malaysia Today*, 6th July 2011; "Anifah summons Singapore envoy over Wikileaks content," *The Star*, 15th December 2011.

malware, worms, Trojans) up to 50% of the cases. Lesser incidents involve malicious insiders (33%); theft of data-bearing devices (28%); SQL injection (28%) phishing (22%); and web-based attacks (17%) [2].

In conformity with the above reports, Bandai (2010) examines that there are many ways to activate data breach [3]. He categorized data threat agents into three, namely "hacker and malware"; "well meaning insiders"; and "malicious insiders". *Hacker* breach is usually conducted in multiple phases including (1) incursion phase, (2) discovery phase, (3) capture phase, and (4) exfiltration phase. The action of *well meaning insiders*, on the other hand, is a key causative factor in a large number of breach cases. According to Verizon Data Breach Investigation Report 2009, 67 percent of data breach reports come from insider negligence. And typical breach cases perpetrated by *malicious insiders* involve personnel with valid access credentials for the data they intend to steal.

Meanwhile in the US, the Industrial Control System Cyber Emergency Response Team (ICS-CERT) reported that there was a dramatic increase in the number of reported cyber-security incidents affecting the U.S. critical infrastructure companies between 2009 and 2011. In 2009, ICS-CERT fielded 9 incident reports. In 2010, that number increased to 41. In 2011, it was 198. The report says that of all critical sectors, water sector is the one most implicated, accounted for more than half of the incidents, as shown by the Figure 1.

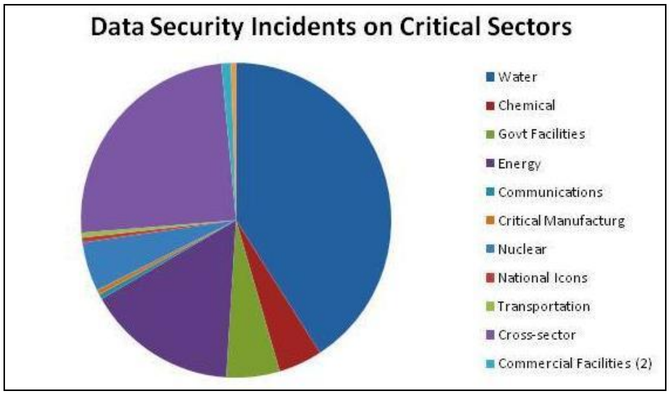

Figure 1. Data Security Incidents on Critical Sectors in the US (2011)

It is increasingly obvious that with new advances of information technology (IT) data breach trends are also growing, potentially beyond control. Hackers would keep improving and reinventing modes of data breach as the technology becomes more and more superior. Worse still, IT security in 2020 will be less about protection from traditional bad guys, and more about protecting business models (in corporate level) or national interest (in country level). As reported by Schneier in Security 2020, that the trends of IT in the year 2020 will be shaped by a few interconnected concepts [4]. First, there will be a *deperimeterization* that assumes everyone is untrustworthy until proven otherwise. Secondly, there will be *deconsumerization* that requires networks to assume all user devices are untrustworthy until proven otherwise. Next, *decentralization* and *deconcentration* will not work if one is able to hack the devices to run unauthorized software or access unauthorized data. *Deconsumerization* will not be viable unless you are unable to bypass the ads, or whatever the vendor uses to monetize you. And *depersonization* requires that autonomous devices to be "truly" autonomous. It is very obvious that all these trends lead to the increased risk of data breach [4].

Data breach issue becomes even more crucial in 'cloud computing' environment. Some IT security professionals viewed the 'Cloud' as the "perfect storm" for data breach. The storm will be technologically facilitated by three factors: mobility, cloud and virtualization. These would be driven by three parallel forces namely *deperimeterization*, mobility and improving data centre efficiency [4]. What was practiced by the Wikileaks in late 2010 was one of the recent examples of the misuse of cloud computing (as serviced by Amazon). Similar incidents occurred in Europe that forced Google to make an apology when its Gmail service collapsed. Salesforce.com had been hit by phishing attack in 2007 which duped a staff member into revealing passwords. In sum, the cloud is becoming particularly attractive to cyber crooks.

## III. Critical Information Infrastructure and Its Difference from Ordinary System

The term CII comprises of three main component; 'critical', 'infrastructure, and 'information infrastructure' [5]. This term has different connotation in different countries. To that extent, a German agency, *Bundesamt fur Sicherheit in der Informationstechnik*: 2004), reiterates that whereas it is possible to identify some common structural elements between countries in terms of the measures taken so far, the functions performed by the responsible organisations and the degree of protection achieved to date remain widely different.

What makes the protection of CII an important national security interest is its 'criticality' criteria. CII is about the reliance of a nation or public to those information assets. It must be the information assets which are so enormously important to the extent that the loss, lack or inefficiency of which would lead to a serious impact.

Countries vary in their perception of how serious is serious. It may involve a "major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life" as defined by the Centre for the Protection of National Infrastructure (CPNI), UK. In the US, criticality is associated with the debilitating impact on security, national economic security, national public health or safety, or any combination of those matters [6]. Based on that factor, in the US, military and diplomatic sectors are essentially critical sectors that house critical infrastructure. In the US, the President's National Strategy for Homeland Security (NSHS), issued in July 2002, views specific infrastructure sectors as critical because of the particular and important functions or services they provide to the country and the fact that its compromise can have a far-reaching effect and potentially reverberate long after the immediate damage. Listed under such critical infrastructures are agriculture, food, and water sectors, public health and emergency services sectors, institutions of government and administration, defense sector, information and telecommunications sector, energy, transportation, banking and finance, chemical industry, and postal and shipping sectors.

The word ‘infrastructure’ literally means “the basic structures and facilities necessary for a country or an organisation to function efficiently.” In many countries, the CII policies cover both tangible and intangible assets as well as production or communications networks. Australia, as indicated by the Attorney General’s Department, for example, covers “physical facilities, supply chains, information technologies and communication networks;” the UK’s Centre for the Protection of National Infrastructure (CPNI) covers ‘essential services and systems including physical and electronic,’ while the US covers the ‘system and assets, whether physical or virtual.’ As a whole, the term ‘critical information infrastructure’ relates information and information assets. In a civil aviation sector, for example, this may include airplanes, personnel, navigation system, information and communications systems, towers and airports, administrative as well as regulatory infrastructure. CII is one part of these: it is all about the information and communications system operated for and by the aviation system. In this respect, the protection of critical information infrastructure refers exclusively to the security and protection of the IT connections and IT solutions within and between the individual infrastructure sectors.

In Malaysia, the Critical Information Infrastructure are defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on Malaysia’s national economic strength, national image, national defence and security, government capability to function, and public health and safety (National Cyber Security Policy 2006 or “NCSP”). The NCSP defines the Critical National Information Infrastructure (CNII) as constituting the ‘networked information systems of the ten critical sectors.’ The ten sectors include national defence and security; banking and finance; information and communications; energy; transportation; water; health services; government; emergency services; and food and agriculture.

From the above discussion one can conclude that it is the critical information infrastructure that makes or breaks national economy. As the network is massive, the points of attacks can be hard to determine. As such one may wonder how invincible the Malaysia’s critical information infrastructure is.

## IV. WHY IS THE CRITICAL INFORMATION INFRASTRUCTURE SO VULNERABLE?

The increasing reliance of critical sectors on the computer networks and information system provides an enormous and unprecedented task. As Condron (2007) described, for the first time in history, an individual armed with nothing more than technical expertise, a computer system, and a network connection could theoretically bring a nation to its knees. The fact that an attack to critical infrastructure is not merely an ordinary criminal matter but rather an issue of national security makes it more urgent for governments worldwide to come up with the necessary policies, plans or laws addressing issues ranging from information sharing to public-private cooperation, from criminal laws to national security, and from public awareness to law enforcement [6].

The protection of CII has been an international concern. The OECD reported in May 2008 that many countries have national plans or strategies start by first identifying what constitute a ‘critical infrastructure’. The concept includes the physical or intangible assets whose destruction or disruption would seriously undermine public safety, social order and the fulfilment of key government responsibilities. Such damage would generally be catastrophic and far-reaching. Sources of critical infrastructure risk could be natural (e.g. earthquakes or floods) or man-made (e.g. terrorism, sabotage).

This concern is natural given the fact that we gradually move into an electronic environment where most documents are being digitised and transactions computerised, such as what is happening with revenue collection and many other government applications. Given such security challenges that face electronic environment such as this, we are left with one nagging question, ‘how secure are those systems?’ The answer to this question will undoubtedly have a huge implication on the life of the community and country as a whole.

## V. IS MALAYSIA’S CRITICAL INFORMATION INFRASTRUCTURE AN IMPENETRABLE FORTRESS?

With the increasing reliance of Malaysia’s critical infrastructure on the ICT, the need to have a secure and resilient information infrastructure is imminent and inevitable. The key objectives of the NCSP declare that Malaysia’s national critical information infrastructure must be secured and resilient, that is, immune against threats and attacks to its systems. The primary question is whether or not Malaysia is ready to address those threats. At this juncture, it is instructive to understand how ‘widespread’ and critical data breach is in Malaysia.

Recent incidents involving public facilities and critical sectors such as railway operation, stock exchange, postal system as well as government agencies have raised concerns over the security of our critical information infrastructure. In one incident, on busy hours in July 2006, the State-linked Light Railway Transit (LRT) system experienced a computer glitch that resulted in the lost of tracking on the monitor screen in the control centre. What follows was a service disruption every five minutes and the trains were running at a much slower pace. Due to a failure of backup system, the situation got worse and caused thousand passengers stranded hours in the trains and at stations. The management quoted an unexpected technical failure as the cause of disruption.

In another embarrassing incident reported by *The Star* on 4th July 2008, a computer system malfunction caused Bursa Malaysia, the national stock exchange, to suspend a whole-day trading. According to the President of the Malaysian Investors Association, such unprecedented interruption to the stock trading was estimated to have caused the Government RM 1 million losses in stamp duty from contracts done while brokers stood to lose RM 5 million. Monetary losses were not the only thing occurred: the Stock Exchange and the Malaysian economy may have also suffered from credibility loss.

There was also a series of unauthorised access and web defacement by anonymous hackers against several government websites, apparently done in concert as revenge to the Government’s latest decision to crackdown websites that are allegedly conducting activities in violation of copyright law

(*The Star*, 17th June 2011). Even though the damage was said to be minor, the fact that it was intentional attack on a national basis indicates that the country's interest may be at stake.

The national agency CyberSecurity Malaysia reported that in the year 2011 alone, there was a total of 15,218 incidents involving online harassment, online fraud, hacking, malicious programs, denial of service and intrusion. This was almost a double increase from 8090 incidents reported throughout 2010 (3564 in 2009). Meanwhile, spamming alone in the year 2011 was recorded at 110,870. This 2011 incidents report is illustrated in Figure 2 as reported by the Malaysia Computer Emergency Response Team (MyCert).

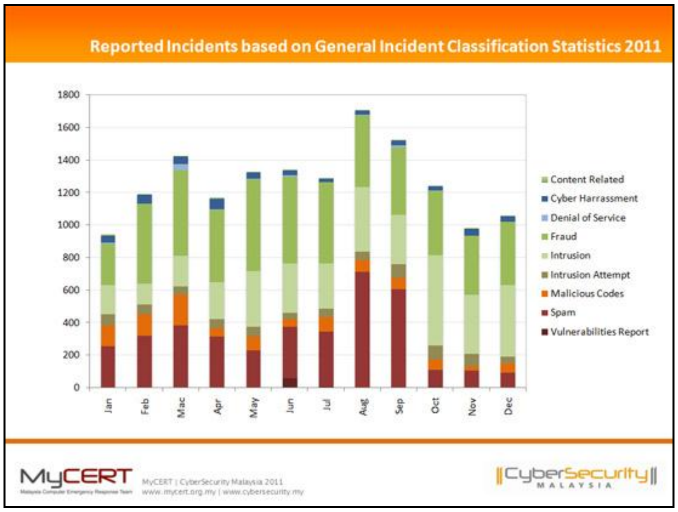

Figure 2. Data breach incident in Malaysia (2011)

Identity theft in Malaysia is also reported as rampant, including personal data abuse allegedly linked with a government agency dealing with university student recruitment in 2005 (*The Star*, 6th August 2005). According to the 2011 MyCert Incident Statistics report cited above, the report of data intrusion and abuses indicates to at least 4,433 incidents took place. All these reports show that data breach is on the increase in Malaysia. The hackers are increasingly becoming more competent, sophisticated and with the lack of knowledge on information security. There is a concern that our critical information infrastructure will not be an impenetrable fortress. If Malaysia wishes to continue its impressive growth, securing its critical information infrastructure is now a necessity because attacks to it can cripple the country.

## VI. CAN THE LAW COPE?

That question had been there for some time [7] on the doubtful ability of law to deal with newly emerging technological threats and challenges. Likewise, on the new and complicated field of CII, the law seems far from ready to face the challenges in a comprehensive way. In fact, many countries including Malaysia do not have a specific law on the protection of CII. It is however noted that several laws may offer limited assistance in dealing with the problems and challenges, notably from the laws that deal with security issues as well as electronic environment.

Security law may be represented in several legislation including the Protected Areas and Protected Places Act 1959, Penal Code and the newly passed Security Offences (Special Measures) Act 2012. While these laws do identify some important concept such as *protected place*; *essential services*, and *essential infrastructure*, they are nevertheless insufficient as they are more designed to deal with tangible assets or physical infrastructure. On the same token, the set of cyberlaws such as the Computer Crimes Act (CCA) 1997, the Communications and Multimedia Act 1998 and the Personal Data Protection Act 2010, suffer from serious limitations. One primary concern is that these laws do not materially differentiate a threat to CII from ordinary computer abuse on private computers. In the instance that such attack took place and the case was dealt with under the current CCA 1997, this means the CII is nothing more than an individual computer system. This wrong message would underestimate the need to protect the security of CII in Malaysia.

## VII. POSSIBLE LEGAL OPTIONS?

As there is no specific legislation that addresses attack on the critical information infrastructure, it would be prudent to see what other nations are doing, especially the US.

### *A. Activating the law of espionage?*

Not surprisingly, using the law of espionage has been considered by the US to prosecute those who leak critical data as illustrated in the Wikileaks saga. This was also suggested by Doug Meier (2008). As it is possible to prosecute the traditional media for publishing government secrets, so it is possible to extend that to the new media. However, as it is too easy for people with classified information to leak it to the public, it is necessary for the government to tighten up its current protocols for protecting its truly secret information. Meier admitted that there are technical problems in tracking down offenders such as anonymity, territorial restriction and the availability of mirror sites [8]. In fact, this was exactly the strategy taken by the US Government. To strengthen the US government powers to take action against data leaks, the Espionage Act was amended to criminalise the 'wilful and knowing' disclosure of 'properly classified' information by any person who is current or former authorized access to classified information to 'any person who is not authorized access to such classified information, knowing that such person is not authorized' such access.

Hester (2011) examined the US government's move to amend the Espionage Act and introduce a new SHIELD ACT in order to deal with the disclosure of government's sensitive secrets more effectively. In his view, such move would further obfuscate the line between the person who leaks intelligence that threatens national security and the person or institution that publishes the leaked intelligence that threatens national security. More worrying, the introduction of this Act indicates that the US government is willing to expand the concept of espionage, without waiting for decisions from the judiciary. That may come in the expense of freedom of press [9].

Therefore it was argued that the US Government should not use their powers to take action against those involved in data leaks indiscriminately. Papandrea (2008) reckoned that in any prosecution against a non-governmental actor for disseminating national security information, the government must demonstrate not only that the disclosure posed an immediate, serious, and direct threat to national security, but also that the offender either intended the disclosure to harm the United States or help a foreign nation, or that the offender was recklessly indifferent to the harm that the disclosure would cause [10].

### *B. A Clash with Fundamental Liberties?*

On the other end of the spectrum, there may be difficulty in crafting the correct provisions as technology is ever evolving. Laws crafted for the real world are ill-equipped to deal with new media. Robinson (2010) conceded that leaks have long been relied upon by the traditional or 'old' media as their source of information and shield themselves under the laws protecting free speech. However, Wikileaks have called into serious question the legal regimes related to the disclosure of information, including protections related to freedom of speech and the press, protection for sources and whistleblowers, the alleged need for confidentiality in government, and the justification for concomitant limitations upon freedom if information and transparency [11]

There is also freedom of expression interest. Michalec espouses that the failure of the government to prevent 'leaks' is not necessarily a failure of the existing scheme, but rather a failure of the government to apply current controls. Michalec argued against the new provision as being an unnecessary, overbroad which would result in the chilling of freedom of expression [12]. Dmitrieva further questioned the wisdom of applying the criminal anti-theft statute to leaks of confidential government information. She raised a number of policy issues on why this should not be done. Top on her list is the concern that the government should not aggressively prosecute against the media for leaking government secrets as this would obstruct the media's ability to conduct independent investigations into the government actions [13].

### *C. Press Freedom in the Public Interest?*

Along the same line of argument, Silver (2008) advanced the view that there must be some form of protection for journalists for disseminating important information to the public. Sharing the same view as others, he shared a profound need to find a balance between national security and the press responsibility to expose the truth [14]. This 'freedom of press' argument has been supported by Lewis [15] but was rejected by Fenster [16] and Peters [17], mainly because Wikileaks indiscriminate disclosure poses more harm than interest. This is because the disclosure has resulted in untold, incalculable damage to the nation's military personnel, national security and diplomatic efforts. Meanwhile Peters opined that Wikileaks is short of a press as it is conducting any investigative journalism. What Wikileaks does is simply dumping of documents. It has not gone far enough to 'minimise harm' by removing the identities of individuals involved in the documents leaked [17].

### *D. Targeting the Intermediaries?*

Some argues that whilst it is difficult to target Wikileaks itself, it is possible to prosecute the person responsible for the leaking. Davidson (2011) opines that in the US, for example, the government was eyeing to prosecute Pfc. Bradley Maning, the US soldier suspected of disgorging unprecedented amounts of classified military and diplomatic reports to Wikileaks. Any restraint action against Wikileaks per se would be futile. If the US government chose to ask for an injunction against Wikileaks, for example, the effectiveness of the injunction would be problematic given its worldwide reach. Removing the Wikileaks materials from the Internet is equally problematic as it appears that the organisation maintains its content on more than twenty servers around the world and on hundreds of domain names. The obvious target is of course the person responsible for the leaks or the leakers as it within the target of the government [18].

Even more difficult would be prosecuting the downstream publishers who obtain the materials from the internet. Enjoining them for further circulating or publishing the materials would pose several legal hurdles. Bella powerfully advances the view that any strategy for shaping the environment for leaks must focus on both the technical as well as the legal environment [19]. There must be a system which access to information is restricted only to the information necessary for the user to perform his or her assigned functions. There must also be tools to detect anomalous data activity from sources inside as well as outside of the affected network and the possible need for insider threat profiling. If such system is not effectively monitored, the environment for leaks has been created.

### *E. Other Options*

For countries with freedom of information legislation, the challenge will be building in restriction of access in relation to national security documents. Lane et al (2008) examined the practices in US, UK, Canada and Australia in ensuring that despite supporting the concept transparency, certain classes of government documents are kept restricted in terms of access. In other words, there must be adequate protection against the disclosure of 'sensitive government documents'. For example, exemptions could be built in for documents the disclosure of which would or could reasonably be expected to, damage the security or defence of a country. Or damage to international relations or divulging information received in confidence by or on behalf of foreign governments or international organisations. This is to guarantee that the functions of government would be impaired, if not crippled and the interests of the individuals and businesses prejudiced. Lane viewed that such exemptions would not create any chilling effect on the operation of the freedom of information law [20].

Lane further pointed out a major problem in protecting 'critical infrastructure', i.e. in that a major portion of it is privately owned or operated commercially. As a result, information sharing between government and the private sector has become a vitally important component of effective risk management. It is prudent thus for a country to establish a platform of cooperation between the owners and operators of the critical information infrastructure within a particular country. In Australia, this comes in the form of Trusted Information Sharing Network which was created in 2003. This platform is created to identify critical infrastructure, analyse vulnerabilities, risks and sector interdependencies and prepare for 'hazards' [20].

Meanwhile a different solution is offered by Freedman (2012). He ventured further to propose treating state secrets as intellectual property as a strategy to prosecute Wikileaks [21]. This is because pursuing a copyright case gives a higher chance of success in comparison to espionage. Firstly, Wikileaks disclosure will not be caught under the fair use exceptions. Secondly, copyright action is hot hurdled by issues of extraterritorial application. Most importantly, copyright received a strong constitutional backing and would not face the limitations and challenges of extradition.

From the US experience, it is clear that laws drafted for traditional media are ill-equipped to deal with problems posed by the new media. The whole experience with Wikileaks suggest that a fresh look at the existing legal framework involving media, whistle-blowing, data leaks, freedom of information, freedom of press and critical information infrastructure.

## VIII. CONCLUSIONS

The widespread of ordinary data breaches in Malaysia demonstrates how real the danger of leakage of government's sensitive data specifically and the critical information infrastructure generally. As the hackers increase in terms of sophistication and technical expertise, and as the critical information infrastructure becomes more massive and intricate, it is more vulnerable to attack.

What would be the legal options for Malaysia? We can tread on the same path of the United States; we can treat the leakers as espionage or worse still, terrorists which justifies grave action under the new security laws. If we take this path, we must be prepared of the consequences. What is more compelling is the need to strengthen the security of the CII itself. As illustrated in this article, a multi-prong action is required; one that involves a mixture of technology, manpower training and effective legal framework.

Finally, it is note-worthy that this initial study raises several issues as ground for future research agenda. Firstly, there is a continuous need to assess emerging methods of data leak and security breaches that potentially threaten the security of critical information infrastructure. Emerging technological trends such as cloud computing, the Internet of things and the intelligent cities would certainly incite new methods of data breaches. Secondly, this study reminds governments to put in place necessary laws or policies to ensure that each sector identified as critical infrastructure be sufficiently protected. On top of that, this study solicits further research on assessing and analysing the existing legal landscape that aims to protect the critical information infrastructure in Malaysia, involving all enabling laws from all sectors. Through such study, gap can be identified and problems be further enhanced.

## REFERENCES

[1] D. Leigh and L. Harding, Wikileaks: Inside Julian Assange's war on secrecy. US: Guardian Books, 2011.

[2] Ponemon Institute, "2011 Cost of Data Breach Study: Global," retrieved from: <http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf> (accessed 15th September 2012).

[3] S. Bandal, "Data breach: Cause, circumstance, remedies," Secure Asia 2010.

[4] D. Howard and K. Prince, Security 2020: Reduce security risks this decade. US: Wiley, 2010.

[5] Bundesamt fur Sicherheit in der Informationstechnik (BSI), "Critical infrastructure protection: Survey of world-wide activities," BSI Kritis, 4/2004.

[6] S. M. Condron, "Getting it right: Protecting American critical infrastructure in cyberspace," Harvard Journal of Law and Technology, 20 Harv. J. Law & Tec 404 2007.

[7] C. Edwards, N. Savage and I. Walden, Information technology and the law. UK: Macmillan Publishers Ltd., 1990.

[8] D. Meier, "Changing with the times: How the government must adapt to prevent the publication of its secrets," The University of Texas School of Law, 28 Rev. Litig. 203.

[9] J. L. Hester, "The Espionage Act and today's high-tech terrorist," 12 N.C.J.L. & Tech. On. 177 (2011).

[10] M. Papandrea, "Lapdogs, watchdogs, and scapegoats: The press and the national security information," 83 Ind. L.J. 233.

[11] J. Robinson, "Wikileaks, disclosure, free speech and democracy: New media and the Fourth Estate," (2012). More or Less Democracy & New Media, 144.

[12] M. J. Michalec, "The classified Information Protection Act: Killing the messenger or killing the message," 50 Clev. St. L. Rev. 455.

[13] I. Dmitrieva, "Stealing information: Application of a criminal anti theft statute to leaks of confidential government information," 55 Fla. L. Rev. 1043.

[14] D. A. Silver, "National security and the press: The government's ability to prosecute journalists for the possession or publication of national security information," 13 Comm. L. & Pol'y 447.

[15] K. Lewis, "Wikifreak-out: The legality of prior restraints on Wikileaks' publication of government documents," Journal of Law & Policy, Vol. 38: 417 [2012] .

[16] M. Fenster, "Disclosure's effects: Wikileaks and transparency," Iowa Law Review Vol. 97:753 [2012].

[17] J. Peters, "Wikileaks would not qualify to claim Federal reporter's privilege in any form," 63 Fed. Comm. L.J. 667 2010-2011.

[18] S. Davidson, "Leaks, leakers, and journalists: Adding historical context to the Age of Wikileaks," 34 Hastings Comm. & Ent. L. J. 27 2011-2012.

[19] P. L. Bella, "Wikileaks and the institutional framework for national security disclosures," The Yale Law Journal, (2011) 121: 1448.

[20] B. Lane, S. Corones, S. Hedge and D. Clapperton, "Freedom of information implications of information sharing networks for critical infrastructure protection," 15 AJ Admin L 193 [2008].

[21] J. Freedman, "Protecting State secrets as Intellectual Property: A strategy for prosecuting Wikileaks," 48 Stan. J. Int'l. L. 185 (2012).