ABSTRACT

This paper investigates the need for Malaysia to relook at and redefine the concept of national security amid the changing circumstances especially in relation to the country’s increased reliance on the information and communications technology (hereinafter, ICT). The more a governance system is exposed to the Internet and ICT, the bigger the risks it would face. When the security of the system is not reliable enough to secure the system, information assets are at stake and the country’s critical information infrastructure (such as defence, communications, energy and medical systems) will become loophole that undermines national security. At the end, the paper examines Malaysia’s policy and legal initiatives it has set to adopt. While steps have been taken to provide necessary policies and strategies, it is argued that the law on national security requires a fresh look and interpretation in order to support the protection of national critical information infrastructure.

Key words: national security, digital economy, critical information infrastructure, law and regulation

Introduction

Security is about preventing adverse consequences from unwanted actions of others (Schneier, 2003). National security, in turn, is concerning the prevention of adverse consequences that may threaten a nation: from all aspects of its life. National security is therefore a broad and diverse concept, ranging from public order to racial and religious harmony, from economic strength to social welfare, from political stability to smooth governance. While this concept of security may remain largely relevant, the understanding needs to be refined so as to adapt with the changing circumstances especially in relation to the country’s increased reliance on the information and communications technology (ICT).

Malaysia, just like many developed and developing countries, has geared itself towards making electronic government and electronic commerce as the main driver of the economy. ICT and the Internet have been largely seen as the main enabler to the governance both in public and private sectors. The challenge is, the more a governance system is exposed to the Internet and ICT, the bigger risks it would face. When the security of the system is not reliable enough to secure the system, huge information assets are at stake and the country’s critical information infrastructure (such as defence, communications, energy and medical systems) would be just another loophole that undermines national security. The recent Wikileaks saga on the leakage of the United States’ secret information illustrates the big problem: when the access to its critical information infrastructure (in this case was its defence and diplomatic cables) can be compromised or abused, valuable and confidential data would leak and cause detriment to the national security.

Taking the sustainability of Malaysia’s critical information infrastructure (hereinafter referred to as ‘CII’) as the focus, the research questions of this paper are of three folds: firstly, what are the risks and threats posed by the digital economy that may compromise its national security? Secondly, has Malaysia as a country put forward national policies that address and aim at the security and sustainability of its critical infrastructure? And thirdly, should there be a reform towards the legal system in Malaysia in order to empower the security of its critical infrastructure? And if the answer is in positive, in what way the reform is to be made? The theoretical concepts that are relevant to frame this research include the concept of national security, the notion of critical information protection and the legal framework on information security.

The objective of this paper is to investigate the factors and circumstances that threaten national security in Malaysia vis-à-vis its increased reliance on the digital technology and the Internet. Simply illustrated, a criminal with a laptop, computing skills and a mini modem can now be more devastating than a terror squad with rifles and bomb in their hands; considering that there are now many more public infrastructure that are dependent on an inter-connected network system. This paper also seeks to assess Malaysia’s readiness in terms of policy and legal framework to deal with these challenges. This paper argues that national security should be given fresh definition and perspective to include the security and sustainability of the critical information infrastructure. It
believes that if sustainability and security is anything to go by in this digital economy, Malaysia and all other
countries should relook on how they manage and secure their information assets and what policies or laws are
put in place to safeguard the situation or prevent abuses.

Revisiting the Digital Economy: Nature and Challenges:

Digital economy is a derivation from a bigger theme ‘Information Age’ where lives an information society
who regards information as the main asset and the most valuable property. It is also where, as Chomsky (1991)
suggested, the politicians battle to control sources of information. It is also the battlefield where technologists’
race to create the most powerful tools and devices to keep, store, process and exploit information—such as what
happens in the Internet search engine and web browser industries. This is where professionals are known as
information workers, and furthermore in macro level, it is where the society is demographically divided into the
information-rich and information-poor. That is the equation of the Information Age.

While the equation is simple, the reality is not always obvious. James Boyle (1997) reckons that the ‘vague’
expression of Information Age is often mistakenly taken by people as primarily a technical incident where only
gadgets change. He warned us that we should beware of the tendency to equate information with computers,
software, and electronics. Information does not need to be stored in ones and zeroes, and those who collect and
manipulate information are not confined to the world of computers.

If the preceding equation is indicative of anything, the most obvious one is that the Information Age is a
discourse of cross-disciplinary matters. No less than information scientists, engineers, lawyers, accountants,
sociologists, political scientists and business people are all concerned. In the word of Boyle, this is called “the
collapse of disciplinary boundaries.” People from different disciplines may end up talking on common subjects.
It is now usual, for example, to see scientists and environmentalists talk about green-houses’ effect; or doctors,
biologists and lawyers talk about biotechnological patent issues; or accountants, lawyers and technologists talk
about online corporate fraud; and many more examples.

On this pretext, too, this paper looks at the re-emergence of the concept of ‘security’ to mean something
multi-contextual: security is no longer physical or territorial, but it should be viewed to include the security of
the national information system. In short, it is both in real and virtual space that security should be assured. Like
what Hornby & Clarke (2003) observed, in a digital economy we can use a set of theoretical perspectives
outlining the recent changes in society to analyze different scenarios for current and future developments in
society. Meanwhile Mackay et al. (2001: 1) asserts that information society is taken as a common conception of
contemporary social transformation. In other words, it is an umbrella term used by various authors and
commentators to refer to a far-reaching social change that is underway.

In a digital economy, economic growth is redefined to indicate a new source of wealth that is based on
information assets. Information is seen as a commodity and therefore, like other commodities, it becomes an
object of trade. This aspect of ‘commoditisation’ of information led Boyle (1997) to argue that “if the shift to an
information society means anything, it means thinking about information as one of the most important resources
in the society.” As Stewart (1997) commented, in this new economy, knowledge has become a primary
ingredient of what people make, do, buy and sell. As a result, managing it – finding and growing intellectual
capital, storing it, selling it, sharing it – has become the most important economic task of individuals, businesses
and nations.

This concern is shared by many other governments, not less by Malaysia. Prime Minister Mahathir
Mohammad –as he then was– strongly acknowledged the crucial role of information and knowledge being the
new basis for power, wealth and influence in the Information Age. For Malaysia, information and knowledge
becomes a new parameter in economic advancement and social progress. He pointed out that the defining
character of a rich or poor country in the future is no longer the state of its industrialisation, but rather the state
of its informatisation (Mahathir Mohammad, 2000).

Threats to Security in Digital Economy:

As pointed out above, the concept of national security should change with the emergence of a digital
economy. The focus that has been placed for a long time on physical and territorial security should now be
widened, not shifted, to the security of the national critical infrastructure and its information system. It is an
increasing and real worry that someone with enough technical skill and malicious minds can bring a nation into
jeopardy by causing problems to its critical information infrastructure.

Such increasing reliance of critical sectors on the computer networks and information systems 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.

To illustrate the problems, the recent Wikileaks saga that puts public hundreds of thousands secret documents from the United States’ diplomatic cables provides how loopholes in the critical information infrastructure are tantamount to damaging situations. When critical data about defense, security and military activities are leaked to wrong hands, national and public interests will be put at stake (Leigh & Harding, 2011). As reported by the Economist (October-December 2010), 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 were 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. In response to the global reaction, the US government considered taking legal actions while at the same time tried to control the damage.

It is indeed a worrying fact that the interconnection that we live by today is not free from risks and threats: deliberate or otherwise, tangible or otherwise. Technical glitches or negligence to the operation and maintenance of the information assets in this aspect could literally be catastrophic. The magnitude of the problem due to the interruption of the information system in the critical infrastructure is best illustrated in several incidents as follows:

- In the UK, a glitch caused disruption to the traffic computerised control system that led to dysfunctional lights across central London and caused long queues on main roads (“Computer glitch causes road jams,” BBC News, 5th April 2009).
- A computer breakdown at Taipei’s international airport caused chaos and long queues, and forced immigration officials to hand-record departing passengers’ data, taking the risk that certain blacklisted individuals or criminal suspects may be let free to flee the country (“Computer glitch causes chaos at Taiwan airport,” Asia-Pacific News, 6th January 2009).
- In June 2007, a computer glitch caused false alarm aboard the International Space Station, prompting mission controllers to run through emergency procedures to try to detect the presence of fire (VOA News, 14th June 2007).
- Financial sectors are not spared either: two groups of commercial banks in Canada were hit with unidentified computer glitches causing about 60,000 personal line-of-credit accounts affected by a system error that in turn caused a double-dipping effect on customer accounts and troubled the online banking systems (IT World Canada, 29th July 2004).
- The incidents of computer glitches or technical malfunction may also be potentially fatal. A faulty computer unit had caused a Qantas jetliner to experience two terrifying midair plunges within minutes on a flight from Singapore to Perth on October 2008. The cause of this incident, which reportedly injured more than forty people, was confirmed by the Australian Transport Safety Bureau (ATSB) in its report few months later (ZDNet Asia, 9th March 2009).
- Singapore experienced technical glitches in its electricity system in 2002 when a computer problem had resulted in the worst blackout in over a decade in the island country. It ultimately paralysed parts of Singapore for ninety minutes and prompted an emergency valve to close, cutting off the flow of the gas to one of two Singaporean providers of the fuel, the SembCorp Gas. The lack of gas consequently tripped seven power plants. As a result, there was an 8% shortfall in the amount of electricity produced (The Straits Times, 15th August 2002).
- In March 1997, a teenager hacked into a telephone company computer that serviced the Worcester Airport, Massachusetts. This caused telephone services to the control tower, the airport fire department, airport security and various other departments to be suspended for more than six hours. The attack caused a ripple effect of delayed and cancelled flights across the country, leading to serious financial losses by the airport and several airlines (Taylor, 2006).
- Similar incidents have hit Malaysia, too, affecting public facilities and critical sectors such as railway operation, stock exchange, postal system as well as government agencies. In one incident, a computer system malfunction caused Bursa Malaysia, the national stock exchange, to suspend a whole-day trading (“Bursa grinds to a halt,” The Star, 4th July 2008). 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 in stamp duty from contracts done while brokers stood to lose RM5 million in the non-trading day. Arguably, these monetary losses were not the only thing incurred: stock exchange and Malaysian economy in general may suffer from credibility losses.

The origin of the above incidents is more of technical and non-deliberate failures; one of many threats to information security. Others come from deliberate acts that may trigger liability under a criminal law. As Grabosky (2007) puts it, the annals of cyber crime now contain examples of successful attacks against air traffic control systems, sewerage treatment facilities, and large electronic retailers, as well as the occasional mail bombing of governmental services and defacement of governmental websites. These attacks can prove more
fatal or catastrophic, and such threats are not esoteric but are real and being exploited on a daily basis, and the consequences of such attacks are significantly harmful.

The Wikileaks and other incidents above raise some causes of concern: firstly, a highly critical infrastructure such as one that houses the military/defense system and diplomatic cables are not spared from security breach or intrusion. Secondly, such breach or leak to the critical information infrastructure (CII) can in turn cause far-reaching damage to public interests, national security or economic sustainability. Last but not least, the problems cannot be quickly or efficiently addressed; the hands of law seem incapable of resolving the problem. The critical information infrastructure would have to be supported by a sustainable policy and efficient legal systems. If it is not to prevent the breach to security, it will work at least to minimise the effect of data breach.

Deciphering Security: the Criticality of National Information Infrastructure:

The leaks posed by Wikileaks should be put in perspective: that those data are critical data to the US government. It takes us further that in order to successfully address the threats to security in this digital economy, the governments should relook at the concept and scope of criticality of national information infrastructure.

In the United States, military and diplomatic sectors are essentially critical sectors that house critical infrastructure. The USA PATRIOT Act of 2001 (P.L. 107-56) defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Furthermore, the President’s National Strategy for Homeland Security (NSHS), issued in July 2002, restates that the rationale for classifying specific infrastructure sectors as critical is 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.

Other countries vary in their perception of how serious is serious. As defined in the UK, critical information infrastructure is the one that 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 (See, the Centre for the Protection of National Infrastructure [CPNI], the United Kingdom.). In Australia, as elaborated by its Attorney General’s Department, social or economic well-being and the security of the nation is the key to the concept of criticality. Meanwhile New Zealand’s definition to criticality is consigned to the ‘great disruption’ (See, the Centre for Critical Infrastructure Protection (CCIP), New Zealand).

In Japan, the Information Security Policy Council terms such criticality is consigned to the ‘great disruption of people’s social lives and economic activities’. Germany on the other hand emphasises on the public welfare and the avoidance of a ‘long-lasting supply bottlenecks, significant disturbances in public security or other dramatic consequences’ (See, the report by Bundesamt fur Sicherheit in der Informationstechnik). Malaysia, on the other hand, views criticality on the “severe impact that may be caused to national economic strength, national image, national defence and security, government capabilities to function, public health and safety” (CNII Portal Malaysia).

The above observation shows that ‘criticality’ has various dimensions but all share the common nature of being the utmost public and national concern. Arguably, the differences originated from different public policy adopted by each country. Therefore they may see a criticality when it involves a high-stake national security, economy, public health and safety, essential government services or even a relatively-less-harmful ‘national image’. Countries put it in their own perspective depending also on the national needs and circumstances. Whereas it is possible to identify some common structural elements between countries, the measures taken so far, the functions performed by the responsible organisations and the degree of protection achieved to date remain widely different. The common message is that the concept of national security has now changed or been extended. It is the criticality of information infrastructure that outlines the utmost concerns of the governments in this digital economy.

Digital Security in Malaysia:

National security is a broad and diverse concept, ranging from public order to racial and religious harmony, from economic strength to social welfare, from political stability to smooth governance. According to Tan (2004), Malaysia’s conception of national security has been influenced by a number of factors: geography, history and Malay nationalism, confrontation with Indonesia, the preservation of the territorial integrity of the federal state, the ‘development as security’ approach and many others.
It is pointed out that the objectives of national security in Malaysia can possibly be to achieve these objectives (Tan, 2004):
- The preservation of the Constitution, including the position of the Malay rulers, Islam and the special rights of the Malays (that is, maintenance of Malay political supremacy) and also the legitimate rights of the other races.
- The preservation of national unity and harmony among the various races (in recognition of the fact that any internal ethnic conflict would be destructive).
- Economic development in the context of a multiracial society in order to strengthen internal resilience (i.e. the strengthening of the ability of Malays to survive in a modern, competitive, globalised world).
- Guarding against internal security threats (such as those from armed communist rebellion, communal conflict and Islamic extremist groups).
- The protection of national sovereignty and the preservation of the territorial integrity of the (far-flung) federal state.
- Maintenance of a stable and peaceful environment in the areas of its strategic interests (that is, in its immediate vicinity, regionally and globally).

The objectives of the national security enumerated above, arguably, are not exhaustive. This policy can grow or change according to the political, social and economic circumstances. The challenges brought about by the networked society such as evident in the discourse of the CII may reshape further the Malaysian national security policy in the future.

Therefore the resurgence of threats to digital security in Malaysia has gained attention in Malaysia’s National Defence Policy (NDP) issued by the Ministry of Defence in 2010. The NDP outlines Malaysia’s main policy, direction and strategies on military role in the Country (See, Ministry of Defence Malaysia, 2010: ii). The Policy states that Malaysia has set that maintenance of the national interest is the core to its sovereignty and independence. In connection thereto, the main objective of the National Defense Security is to protect and secure Malaysia’s area of interest from any threats either from abroad or domestic. In relation to the digital security, it confirms the fact that in the Information Age, it is crucial to secure information resources in order to preserve the country’s independence and sovereignty (Ministry of Defense, 2010). It is therefore critical to secure the National critical sectors with upgraded capabilities in terms of cyber defensive and offensive strategies. It is argued here that the inclusion of cyber-security element in the NDP is a good indication, albeit still lacking depth and elaboration. This will have to be developed further to transform the notion of defence and security in Malaysia.

However, a look at the state of digital security in Malaysia may suggest that the transformation of security should take place sooner rather than later. This is because in Malaysia, information security incidents can be seen as a regular casualty on Malaysian computers and computer systems. According to the report by the CyberSecurity Malaysia (formerly known as National ICT Security Emergency and Response Centre or NISER), in the year 2008 alone, there was reportedly a total of 2,123 incidents involving online harassment, online fraud, hacking, malicious programs, denial of service and intrusion, over a hundred percent increase from the 1,038 incidents reported throughout 2007 (1,372 incidents in 2006). Meanwhile, spamming alone in that year recorded more than 80,526 incidents, over a double rise from 38,601 spam reports in the previous year (22,880 in 2006) (2009 Incident Statistics by the Malaysian Computer Emergency Response Team). The figure keeps increasing in 2010 as shown in the diagram 1.

![Diagram 1: Information security 2010 incidents statistics in Malaysia (Source: MyCert)](image-url)
Other than that, cases of information theft are reported in the press on a regular basis. This includes incidents such as old folks who discover someone has been withdrawing their Employee Provident Fund (EPF) savings, families who are told their land is registered under someone else’s name and people who discover someone has been borrowing under their name (The Star, 15<sup>th</sup> March 2008). These cases often took place due to a compromise or loss of some personal data. In one instance, confidential information and personal identity were at the centre of an illicit trading allegation. This includes a claim that confidential student data at Malaysian public universities’ admissions unit was being traded to some private colleges and was then used by the latter to solicit potential students who failed to get places in public universities (The Star, 6<sup>th</sup> August 2005).

In another report, it was revealed that people employed by developers, banks, telecommunication firms, utility companies and car distributors were selling database containing personal particulars of their clients to third parties such as property agents, salesmen and contractors. A complete list of buyers for a luxury housing scheme in Kuala Lumpur areas can easily fetch up to RM13,000 (The Star, 10<sup>th</sup> August 2005).

Those series of lost, stolen or compromised personal data should not be viewed as an incident of its own and therefore would stop there. Instead, these incidents provide ammunition for further crimes: the creation of fake credit cards or impersonated bank accounts and the launching of purchases afterwards, using those fake credit cards or impersonated accounts. It was revealed that a syndicate specialising in making purchases with credit cards obtained with genuine but stolen personal particulars has raked in more than RM1 million in profits in the period of one month in July 2005 (The Star, 15<sup>th</sup> August 2005). Recently it was reported that scams targeting electronic banking have increased drastically in the country, with the number more than doubling over the past year. A total of 1,426 reports were made to CyberSecurity Malaysia in 2010 compared with 634 in 2009 (The Star, 16<sup>th</sup> February 2011).

There are no clear statistics for specific information theft offences in Malaysia so far. In 2004, there were 606 cases reported under the Computer Crimes Act 1997 involving losses at nearly RM 2 million while there were 149 cases reported under the Communications and Multimedia Act 1998 involving losses of RM 630,000.00. Meanwhile in 2005 (January to October), there were 283 cases under the Computer Crimes Act 1997 that involved losses at RM 1.2 million; and 58 cases under the Communications and Multimedia Act 1998 involving losses of RM 294,000. So, there is a drop of 48 percent between 2004 and 2005 (Berita Harian, 19<sup>th</sup> November 2005).

In agreement with the reports above, national consumer associations argued that data security and ID theft are becoming more serious. The National Consumer Complaints Centre receives around 20 complaints involving identity fraud a year; a figure which is increasing (The Star, 15<sup>th</sup> March 2008). This presupposition does not seem unlikely since Malaysia has been identified to host more infected personal computers than any other city in the Asia-Pacific region, making Kuala Lumpur the ‘honeypot’ for hackers (The Star, 17<sup>th</sup> April 2008).

**Policy Initiative in Malaysia:**

Malaysia as a fast-developing country increasingly adopts information technology and computer networking in almost all sectors of its development. It is clearly stipulated in the latest national development plan (the 9<sup>th</sup> Malaysia Plan), which emphasises that a greater adoption and usage of ICT will become strategically more important. The country will need to increasingly harness ICT to improve productivity and competitiveness as well as progress to high value added and knowledge-intensive economic activities. The Government will build upon and enhance ICT capacity for ubiquitous access, develop core competencies, narrow the digital divide and expand usage of electronic transactions as part of the overall effort to empower the populace to partake in the growing networked economy. Simultaneously, this will allow for the greater expansion of ICT-related industries and services (The Ninth Malaysia Plan: 141).

In order to realise this, it outlines, among others, information security as the focus in this period of development. For that reason, “efforts will be intensified to improve information security in order to enhance confidentiality, integrity and availability of online information systems” (The Ninth Malaysia Plan: 152). On top of that, the aim is to enhance the integrity of networked systems, increase trust and confidence in online mechanisms and improve quality of services, among others, through compliance with information security management standards and best practices. In particular, these aspects will be of specific importance to the agencies operating the critical national information infrastructure (The Ninth Malaysia Plan: 153).

It is noteworthy that the Plan makes a specific stipulation and places a specific emphasis on the protection of critical national information infrastructure. Nevertheless, this emphasis has not been backed up by a specific legislation or legal instruments that comprehensively address all the elements of CII. Instead, the Government of Malaysia in 2006 has set up a national policy in the form of the National Cyber Security Policy (NCSP), which is closely related to the protection of national critical information infrastructure albeit emphasis given on a more restricted context of cyber security.
Under the NCSP, 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 (See, the National Cyber Security Policy 2006).

With this definition, the Policy has identified ten critical sectors in Malaysia, i.e. national defence and security, banking/finance, information and communications, energy, transportation, water, health services, government, emergency services, food and agriculture. The NCSP declares its objective that Malaysia’s national critical information infrastructure must be secure and resilient, that is, immune against threats and attacks to its systems. Nevertheless it is argued that several issues require proper attention such as the public-private cooperation, clear job distribution, and transparent national system as well as social and industrial awareness.

The inclusion of private sector is imperative. It was emphasised that approximately 90% of national critical infrastructures are actually in the hands of the private sector. Those companies are also arguably best placed to assess what systems and sub-systems within their own business require special protection. Therefore, it is more strategic and effective for the purpose of control and enforcement.

There is an urgent need to avoid duplication or overlapping of functions between organisations and agencies. Therefore, clarity of functions, responsibility and procedures (such as procedures for information, cooperation and reporting) is essential. On the other hand, there is also an important prerequisite in the form of transparency of the national system for the protection of a state’s own critical infrastructure. Central in this issue is the availability of freely-accessible information.

Last, but not the least, proper awareness at all levels of industry, state and society is a must while sectoral cooperation and international cooperation are a matter of urgency as critical infrastructure protection should not stop at the public frontier or national border only.

Law on Internal Security: Proposition for CII Protection:

Putting law on new technology is not always simple. In the US, for example, Doug Meier (2008) suggested that there are technical problems in tracking down offenders such as anonymity, territorial restriction and the availability of mirror sites. This difficulty is exaggerated by the fact that national security is often vague in terms of its scope. There is a traditional view saying that national security should be handled by the authority in charge and should not be the subject of public sentiment (See, The Zamora’s case [1916] 2 AC 77). In that case, Lord Parker said that “those who are responsible for the national security must be the sole judge of what the national security requires.” His Lordship also said that it would be obviously undesirable that such matters should be made the subject of evidence in a court of law or otherwise discussed in public. This approach is arguably controversial as it could be interpreted that national security matters are arbitrarily decided in the hands of those in power.

In Malaysia, the discourse on national security law in the context of critical information infrastructure protection hardly exists. In many literatures and commentaries, the concept of national security has been linked to constitutional rights or issues of preventive detention. The main legislation on this area is the Internal Security Act (ISA) 1960 (Act 82) although there also exist other laws that serve the objective of public order and national security.

Though the ISA 1960 has never been framed on the issue of critical information infrastructure, this paper views such as important because the law should be given a fresh look in the context of security in a digital economy. It will be examined here to what extent the law can help in the protection of national critical information infrastructure.

In general the Act provides for preventive detention, the prevention of subversion, the suppression of organized violence against persons and property in specified areas of Malaysia, and for matters incidental thereto. In its preamble it stipulates that the Act is made pursuant to Article 149 of the Federal Constitution, with the aim of stopping or preventing actions, prejudicial to the security of Malaysia, that are (1) to cause, and to cause a substantial number of citizens to fear, organised violence against persons and property; and (2) to procure the alteration, otherwise than by lawful means, of the lawful Government of Malaysia established by law.

Having a reputation of being a draconian security law, the ISA 1960 originates from British colonial rule and was intended to curb communist insurgents. Nevertheless this Act has now been used beyond this. It has been used by the Malaysian authority to deal with threats prejudicial to public order and national security of the country. There have been sharp and continuous criticisms on the powers given by this law such as detention without trial up to two years. Unsurprisingly, calls to have it repealed or abolished have been continuously voiced out by various sections in the society (Abdul Aziz Bari, 2003).

Nevertheless, this paper does not make attempt to comment on those controversial debates as these are outside the scope of the study. Instead, it maintains a view that in so long the ISA 1960 still exists as the law in force, it can be used for the protection of critical information infrastructure in Malaysia. The assessment here
A hypothetical situation where section 8(1) of the Internal Security Act 1960 empowers the Minister to order a detention of a person is considered to safeguard the critical information infrastructure. Given this proposition, one can say that rumour-mongering emails can serve to minimize the threat to the critical information infrastructure in Malaysia.

It is argued that this proposition should be looked at by the authority in charge so that it can help prevent or at least contain any threats to the CII. The preventive detention order can constitute a very important instrument to prevent attack on the CII. It is argued that this preventive detention order can constitute a very important instrument to prevent attack on the CII. It is clearly stated that a detention order can only be made with a view to prevent that person from acting in a manner prejudicial to the maintenance of essential services therein or to the economic life thereof, he may make an order (hereinafter referred to as "a detention order") directing that that person be detained for any period not exceeding two years.

While the Act is silent on the meaning of 'security' and 'economic life', it details further the scope of 'essential services' to mean 'any service, business, trade, undertaking, manufacture or occupation included in the Third Schedule' (section 8[2]). The Third Schedule of the Act provides reference of 'essential services' to water, electricity, public health, fire, prison, postal, telephone, telegraph, radio communication (including broadcasting and television), port, dock and harbour services and undertakings, public transport services by land, sea or air, and lastly, bulk distribution of fuel and lubricants (Third Schedule). On a quick look at these 'essential services', one can see similarities with the 'critical sectors' outlined under the country's National Cyber Security Policy (NCSP) discussed earlier, though no attempt or study has been made to compare the two.

It is observed that this rule on preventive detention, despite heavy criticism on constitutional and procedural grounds, can serve to safeguard the critical information infrastructure. Given this proposition, one can say hypothetically that section 8(1) of the ISA 1960 empowers the Minister to order a detention of a person if he is satisfied that such detention is necessary with a view to preventing him from acting in any manner prejudicial to the maintenance of any service, business, trade, undertaking, manufacture, or occupation in the 'essential services' which similarly cover major parts of the 'critical infrastructures'.

If a person, hypothetically, is found to be a threat to the integrity and availability of the information and communication network within the national aviation system—an essential service under the ISA and one of the critical sectors under the NCSP—thus prejudices or causes damage to that system, the Minister can arguably issue a Detention Order under this law against such person to prevent that information security threat. In other words, this preventive detention order can constitute a very important instrument to prevent attack on the CII. It is argued that this proposition should be looked at by the authority in charge so that it can help prevent or minimize the threat to the critical information infrastructure in Malaysia.

Interestingly, there have been arrests and detention taken by the Malaysian authority in cybercrime-related incidents that mainly involve the allegedly-abusive content prejudicial to public order such as in the cases of rumour-mongering emails (The Star, 18th December 2002) and SMS spreading (The Star, 30th August 2007) as well as the posting of offensive blog articles (The Star, 24th September 2008). However, the extent to which preventive detention is used for protecting the CII is so far unknown. It is argued that the Authority should consider applying this law in CII-related incidents especially since it affects real and genuine threats to national security and public safety.

From the above discussion, it is argued that the controversial Internal Security Act 1960 is still useful to address the threats to the national Critical information infrastructure, albeit the need to reinterpret it in a way accommodative of the objective of CII protection. Nevertheless, it has to be born in mind that this law, when drafted did not have the same situations as posed by the security threats in the digital economy today. Further reform is indeed imperative and this has to be done in concert with the reform of other laws on crimes, cyber crimes, terrorism as well as law on protected places. Indeed, the law discussed in this paper reflects only partial issues of the legal reform needed.

Conclusion:

It is imperative to remember that security is a process not a product. Pipkin (2000: 14) reckoned that security is a process of reducing risk or the likelihood of harm. Therefore it has to adopt changes and requirements brought about by the society we live in. In the digital economy, the need for security has become greater due to the peculiarity of security threats in this networked environment. For now, the potential deadly threats to the security of critical information infrastructure may still look unlikely. This situation however should not be a reason to be sceptical, lenient or complacent. It is observed that this current position is not a static situation as the vulnerability of critical information infrastructure to cyber attacks could change with the increasing use of network technologies (Lewis, 2002: 11).

Malaysia should not be complacent especially for two main reasons. First, the security of its critical infrastructure is a vital determinant for national security, thus it should not be taken lightly, leaving the security
to chance—or worse to the hands of malicious criminals. Efforts to strengthen the security and resilience of the nation’s critical infrastructure should be made a priority. Secondly, the advances of technologies and the rise of digital citizens in Malaysia form a part of a global network that seek to globalise everything from business to governance, from friendship to professionalism, and –unfortunately- from crime to terrorism. These would soon present a huge challenge to all those who are dependent on the technology and the information assets.

The policy and legal measures that are discussed in this paper arguably constitute as part of a bigger framework to secure Malaysian critical infrastructure. The law is only one element as other components—technology, standards, public-private cooperation and the institutions—are worth considering, and require further research as well as strategic development. By way of analogy, while it is correct to regard information as ‘oxygen’ for the people and democracy, this paper firmly believes that the critical information infrastructure or CII is the ‘respiratory system’ in which such oxygen is utilised, processed and acted upon.

References

Meier, Doug (n.d.): ‘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.