

## **INFORMATION COMMUNICATION TECHNOLOGY AND THE QUESTION OF STATE SECURITY : THE MALAYSIA EXPERIENCE**

Zaini Othman

International Relations Program University of Malaysia Sabah

[zo@ums.edu.my](mailto:zo@ums.edu.my)

**Abstract :** In the modern age, the increasing use and exploration of information technology and the internet by hackers has created a new security threat to the integrity and socio-political stability of the Malaysian nation. Malaysia is not only one of the most dynamic developing countries in the region, but it is also facing many border disputes and terrorism with its neighboring countries. For example, maritime and territorial disputes between Malaysia and Indonesia, Malaysia and Philippines, as well as sovereignty disputes with Singapore over part rocks island with Singapore. These disputes not only dragged diplomatic diplomats among the two political leaders of the country, but also involved cyber-hacking between countries. For example, cyber-attacks have taken place, when disputes over ownership of the Ambalat Block and East Ambalat Block in the Makassar Strait are at its peak between Malaysia and Indonesia. The attack has resulted in severe damage to a number of government sites owned by both countries. This paper analyzes the emerging role of information technology, the internet and hackers as a potential future security threat to the Malaysian nation and society, both international and domestic.

Keyword : Information Communication Technology, State Security, Malaysia Experience

### **INTRODUCTION**

Terms such as cyber power, the internet, virtual space, and information communication technology (ICT) have, in many cases, dominated the lives and social systems of the world to date. The political system of a society is also no exception from the dominance and influence of these terms especially ICT. For example in the context of a democratic system, the dissemination of information has form as an important element or a fundamental condition for the healthy development of democratic polity and values to be flourished within such democratic society. Hence, the definition of democracy would be incomplete without the freedom of information, the elements of transparency, the freedom of the press and other media as well as various issues related to the basics of information such as level of literacy within society, better access to the education and systematic improved of IT infrastructure.

Thus, this has made the mosaic of community in managing their daily activities becoming more dependent on ICT than ever before. Half a century ago, these phenomenon was something that had never been anticipated; except to specific individuals, groups who have direct links to the science of fiction. One of the most obvious things in the context of these developments is the emergence of a new form of power called as cyber power; which in many cases has a strong influence and dominance on the development of a state societal and public system, particularly on the aspect of security. The unprecedented reliance on computer systems and information technology has brought a new form of threat to the well-being of nations, especially in terms of political stability. For example, cyber threats or cyber warfare launched by one country over another; similar threats may be faced by specific individuals or groups in one country against particular parties located in another country; carried out on specific motives or with specific agendas and purposes through a network of computer systems.

Imagine, our society or country in the future: a certain group or group of people who are well-versed in computer knowledge, called HACKERS, disrupting central electric power computer systems; making false alerts to the country's traffic system; and then sent the news via e-mail and short message to the public mobile phone saying that the government had circulated an order for everyone not to leave their home until a notice was issued? Given consideration on the mosaic and culture of life to date that heavily rely on ICT as well Computer Networking System (CNS), it is very likely that in the near future the same phenomenon will take place in our society. Case in point is most of the critical infrastructure (in modern nation state to date) such as banking and financial systems; power supply; telecommunications and information; gas and petroleum production; transportation; water supply; emergency services; as well as the public service are very much associate with ICT and CNS.

This paper aims to study and analyze the role of HACKERS as a potential new form of threat to the future survival of our nation and society. In doing so, this paper will distinguish three types of activities often used by hackers in the context of security threats to a country's ICT and CNS network system. First, demonic activity refers to any form of action or action that is defamatory or offensive to the computer system of a company, group or government that reflects the conduct of a protest against the activity of that company, group or government. Second, Cyber-terrorist activities are defined as premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-nationals groups or clandestine agents. Third, Cyber-War, refers to the activities carried out by hostile hackers and illegal encroachment on computer systems and networks.

**DISCUSSION*****Hackers, Cyber-Terrorists And Cyber-War: Defining The Parameter***

Hack is an act or action that is falsely accused or intruded into a computer system; whose actions are based on political and social motives. Individuals who perform these 'actions' are called *hackers-activists*. They are very knowledgeable about the intricacies of computer systems. Hackers are completely different from *hackers-activists*. The average hacker is acting out of desperation by wanting or finding out; while the *hackers-activists* are working to persuade the world community that their behavior is civil-disobedience in nature (Michelle. 2017). The activists carry out their own acts of aggression either alone or in cooperation with the idol activists who have the same goal of fighting each other, whether politically or socially. The earliest idea of the term *hackers-activist* was first coined by John Perry Barlow, co-founder of the Electronic Frontier Foundation in 1996 in his declaration on "*Independence of Cyberspace*".

In the modern world to date, "extreme" exploitation of information technology and internet by hackers, as mentioned earlier, has created a new threat to the internal integrity of a nation. Activists see cyberspace as a way or tool for non-state actors to enter into the arena of conflict, whether national or international. In recent times, hacks has emerged as a global phenomenon and is so common in the context of international IT and internet systems. Hack has covered many aspects of attacks in the context of cyber-space; all of these attacks are the result of acts of hacks that are politically motivated, jealousy-nationalism, excitement, curiosity, profit and personal revenge.

Based on recent developments, hacks has become a very popular "ism" of cyber-world or cyber-media and has many followers. This is due to the unprecedented and rapid growth of the Internet in all parts of the world. For example, in the Asia-Pacific region, telecommunications networks have grown so fast that their size has expanded over the last 5 years and is expected to grow over the next 5 years. In this context, the threat of cyber-war is a real and very serious issue for every nation in the region. For example, Malaysia is one of the countries in the Southeast Asian region that is very advanced in terms of telecommunications network infrastructure, ranked 2nd, after Singapore, and ranked 27th in the world in 2016. However, in terms of information technological access, Malaysian covers only 42.2 per cent; that is, by comparison, much lower than the rate of information technological access of the people in the countries such as Singapore, Japan and South Korea; which covers up to 60-70 percent of users (Auerbach & William, 2000).

The Asia-Pacific region is not only a dynamic region in terms of technological development, population, and economic growth; but also a region that is flooded with international conflict among countries in the region, as well as other political power-house from different region. Among the escalations of international conflict disputes that have been

around for decades are the Kashmir conflict between India and Pakistan, the “*Bangsa-Moro*” nationalist separatist movement in the Mindanao region of Philippines; maritime border disputes between Malaysia and Indonesia, Malaysia and Singapore; and the most popular is the Spratly Islands rights dispute involving many countries in the Southeast Asian region as well as countries in East Asia such as China and Taiwan. The aforementioned conflicts have not only been around for a long time and have involved diplomatic disputes among political leaders between countries, but have also involved conflict over the inter-state hackers (Barlow, 2006.).

For example, the conflict between the Moors and the Philippine government as well as the Indonesian Islamic Movement [JI] with the Indonesian government; the 2 supporters of the organization have committed cyber-attacks as well as cyber-crimes against their respective governments; as a form of attack and threat in the struggle of these organizations. This situation was once described by Winston Churchill during World War II as the “Wizard War”. This means that the phrase “Wizard War” revealed by Churchill half a century ago [during the Second World War], has re-emerged in the form of cyber space as a new field or battlefield. In other words, wherever there is a physical or conventional conflict between nations, there will be cyber conflict between the hackers of the country involved ().

One of the most popular forms of cyber-attacks among hackers is the website defacement. The act or deed of damaging the enemy's web site is one of the forms of hacker war activity; where the enemy's web site will be destroyed; and this action is not confined to a specific location or boundary; it is common for activists to carry out their actions or attacks from various locations and levels. Because the internet world is not in a physical state or has a specific physical location, any individual, group or organization that is activist can attack the enemy from any location. For example, a cyber-attack campaign aimed at destroying the website occurred during a dispute between the Malaysian and Indonesian governments over the issue of ownership of the Ambalat Block as well as the East Ambalat in Makassar Strait in 2005. As tensions escalated between the 2 countries, cyber-attacks on the website of Malaysia also increased significantly. Malaysian websites have received attacks and their content has been destroyed. Websites owned by the government administration also received attacks accompanied by insults and hate speech against the government. The Malaysian Computer Emergency Response Team [MyCert or Malaysian Computer Emergency Response Team] reported that 256 Malaysian websites had received attacks and hacked in the first quarter of 2005, compared to 42 websites in the first quarter of the previous year. Among the high profile websites that were hacked in the attack were the Malaysian Multimedia and Communications Commission [MCMC] and the University of Science Malaysia [USM] website.

Malaysian activists have carried out counter-attacks and have successfully hacked 36 Indonesian websites and among Indonesian high profile websites being hacked and destroyed including Indonesia's Department of Homeland Security. However, there is a skeptical side to the cyber-attack. This is due to ambiguous nature of the cyber community such as the anonymity, has made it difficult for the analysts to point precisely that the cyber-attackers on the 2 websites of the country are Malaysians or Indonesians. (Devi, 2017). Based on the expert's analysis of the cyber-attack; they concluded that the attack was unintentional and unprofessional. The attack was according to experts solely in the wake of activists; that is, they do not receive support or assistance from the governments of the 2 countries involved. The issue of Ambalat, is not the first incident where a Malaysian website was hacked or attacked and destroyed. It is well known and well understood that the level of security of the Malaysian internet is not in a secure and reliable condition. For example, in June 2015, activists sympathetic to the Kashmir independence struggle launched a cyber-attack and destroyed the Malaysian government's website. The attack is a manifestation of how cyber space and ICT influence can threaten a country's defense system at any time (Devi, 2017). Meanwhile, terrorist organizations as well as radical organizations use information technology and the internet for various purposes; these include the process of identifying and training new members of the group, planning acts of terrorism and propaganda campaigns. Cyber-terrorists tend to resort to cyber-attacks as a method of attack because it gives them many advantages, including:

1. Cheaper than traditional method;
2. Cyber terrorist activities or actions that are difficult to detect;
3. This method is able to protect their activities from being detected by the authorities;
4. Able to do activities wherever they are;
5. This method is capable of targeting larger goals.

Thus, the information technology revolution that is affecting the world today, provides similar opportunities for terrorist organizations operating in the region to intensify their struggles and activities. For example, a thousand terrorist organizations in Southeast Asia, have used and manipulated the internet in their ideological dissemination activities to the public in the region. These developments indirectly exposed the threat of political stability to countries in the region. Armed terrorist groups are no longer just rifles and bombs; now the weaponry of these groups includes mini-cam, video-tape, CD-ROMs', laptops, CD-Burners, e-mail accounts, and including the construction of specific website.

Two well-known terrorist / radical groups in the region, Abu-Sayyaf and JI, are among the groups that are actively using the internet and IT as the new "weapon" to achieve their goals. JI, for example, was the earliest radical group in adopting IT and the Internet as a tool for the struggle and propaganda of the group, in particular the agenda of spreading the

Islamic Caliphate. Apart from Abu-Sayyaf & JI, the LTTE was once among the terrorists responsible for carrying out a series of cyber-attacks against the Sri Lankan embassy's worldwide computerized computer network in 1997. Using the message "we are the Internet Black Tigers and we are doing this to disrupt your communications", the LTTE has successfully disrupted the Sri Lankan embassy's computerized computer network, and the message clearly proves they were responsible for the hacking activities way back in 1997 (Arquilla & John, 2016).

In light of the recent rapid developments in the cyber world, it is not surprising that today, most countries in the world today are developing and implementing cyber strategies to suppress and destroy their enemy's defense structures. Cyber-warfare is seen as a form of military power deployment that can act as a multiplier. Small-sized countries that have been unable to match the powers of conventional powers, have now begun to move towards developing and strengthening their IT and internet facilities. In the Asian region, for example, China is seen as one of the most active countries in developing their cyber warfare facilities and infrastructure; and this development is seen as a threat to the security of other countries in the region.

### **Information Technology & Security Threats: The Malaysian Experience**

As explained at the beginning of this discussion, this paper attempts to discuss how this development of IT has had a profound impact on a country's political viability and security, especially in terms of security. It is well known that freedom of speech in Malaysia has always been controlled and influenced by the government, but with this development (and coincidentally supported by the government itself with the construction of the MSC) has accelerated the development of democracy, especially in terms of democratic space. Malaysian Prime Minister Tun Dr Mahathir Mohamad could be considered the person responsible for this development as he seeks to enhance the use of IT in the community by launching a project called the Multimedia Super Corridor (MSC). The project is an attempt to develop the use of IT as described by Asian Wall Street Journal as follows:

*"It is Dr. Mahathir who is most responsible for making the Internet accessible to ordinary Malaysians. In 1996, the technology-loving premier launched the Multimedia Super Corridor, an ambitious plan to wire a strip of real estate with telecommunications powerful enough to support "smart" schools, a paperless government, telemedicine and a center for software development, among other things (Asian Wall Street Journal 30 March 1999)."*

In this regard the government under his administration has also doubled down on this agenda. For example, in 1997, the government launched an IT use campaign among citizens across the country. In order to improve the raising awareness of the peoples towards the

use of IT, government through programs broadcast on television, has play-down several slogan such as “accept IT”, “learn IT”, “use IT” and “love IT”. The Internet in Malaysia has evolved since the early 1990s. IT is not only subject to internet and email but also involves many other information technology tools as mentioned above. This effort appears to be fruitful with the increasing number of people using this service. Out of the total 2 million people surveyed, it was estimated that in 1999 an estimated 480,000 people were using the internet and this number is increasing over time (AWSJ 30 March 1999).

The presence of the internet has facilitated the dissemination of information to various parties including governments, political organizations and individuals. Political parties have leveraged this ICT by building their website and sharing a wealth of information as well as providing a wide range of interaction and views. Activists and the public can communicate with each other more quickly and efficiently. However, the use of IT has grown exponentially in the wake of the arrest of former deputy prime minister [TPM] of Malaysia Anwar Ibrahim and the rise of a *Gerakan Reformasi* [Reform Movements] in Malaysia. Reports from the international media say that ICT was fully utilized by his supporters [Anwar Ibrahim] to expose to the public about the movements:

*At 9 pm on September 20, 1998, when masked policemen armed with submachine guns stormed into the home of Malaysia's sacked Deputy Premier Anwar Ibrahim, it was not the local television stations or even CNN which were the first to break the news of the historic arrest. Just minutes after the arrest, an email alert from a supporter present at the house was sent out to newsgroups and discussion lists on the Internet, giving thousands of Malaysians access to vivid details of the events that night. It signaled a crucial turning point in Malaysia's political landscape--the Internet had arrived (Sabri Zain 6 Ogos 99).*

Since then, various sympathetic and supportive sites that support the former TPM leadership have been built on the internet. The numbers are huge and difficult to calculate. Since September 2, 1998, the date on which the former TPM was detained for the first time, over 50 internet sites have been created to provide alternative views to the mainstream media. A spokesperson for TMNet (Malaysia's largest internet service owner) said that previously, only about 9,000 new applications were received per month to subscribe, however, since the TPM detention case, applications for internet subscription purposes have increased dramatically by an increase of 14,000 per month (AWSJ, March 30, 1999). The average new customer is a supporter of the *Gerakan Reformasi* in Malaysia. In the early stages of the movement, among the first sites to be established were *Anwar.com*, *Anwar on-line*, *Reform Page*, *Conspiracy*, *Reform.com* and *Anwar org*. When most of the daily newspapers run by the ruling party made various nasty statements that demeaned Anwar Ibrahim's leadership, widely regarded as the idol of the public, *Anwar Online's website* was set up just two days after his arrest to deny all allegations and highlight their truth. (AWSJ,

March 30, 99). A few days later dozens of new sites were created specifically to give birth to the same aspirations.

With the advent of various web pages the focus of IT is growing. Visits are becoming more frequent and information disseminated is ever-expanding, constantly updated and up-to-date. Suddenly, the public's response to the local press has been declining. Information obtained from distributors of mainstream newspapers around Kuala Lumpur states that for the period 1998-1999, the response and sales of *Utusan Melayu* (The Malay Post) and *Daily News* have decreased by 40%. The public is beginning to feel uneasy with the local newspapers that are seen to be biased. Some of the news published by mainstream newspapers has questioned the validity of the news. For example, news of the gathering of the reform movement was attended by tens of thousands, but mainstream newspapers in their news reports said only a few hundred were present. This question marks the truth of the news reported by the mainstream newspapers. This can be viewed from the excerpts obtained from some of the following sites:

*"Just by looking at a reformasi site, you are making a statement that you reject the mainstream media," says Sumitra Visvanathan, 30, Webmaster of Saksi.com, or "Witness." Photographs and eyewitness accounts on Saksi of the 40,000 to 60,000 strong crowd that gathered in the capital to hear Datuk Seri Anwar the day he was arrested attracted 20,000 hits the day they were posted, says Ms. Visvanathan. She says Saksi isn't strictly a reform site: "We don't glorify Anwar and we don't just knock Mahathir."*

For example the *Justice Page* was built in respond to and compete against pro-reform sites but it did not get good support. A May 1999 report stated that the site received only 18,000 visits compared with those who supported the reform. To date, the so-called *reformasi* supporters have reached more than 200,000 visits, far exceeding the *Justice Page* (New Sunday Times 23 May 1999). Email especially mailing-list is also a growing electronic link in line with IT developments such as *SangKancil*, *Titiwangsa*, *Anwar-net*, *Hizbi-net*, *Fair Net*, *Sarawak Talk* and *News-Malaysia*. It has emerged as a field of free expression. These opinions will be read by others and will be commented or answered so that sometimes it leads to long arguments. In *SangKancil* for example, political, economic and social issues are the main issues in the discussion. There were also discussions about religion in particular Islam and it attracted many commentators including from other religions. What is certain is that the customer here must be moderate in their intellectual views, otherwise they can be easily disturbed or challenged by other people's perspectives on their religion. There are also mailing lists where customers are only provided with up-to-date information on things like *STRATFOR.COM's Global Intelligence*, *Financial Time news*, *Global Knowledge Development (GKD)*, and *Malaysian News*. These IT developments reveal something that has never been disclosed before, served as a counter view or information

---

counter to the mainstream media, and increased public transparency. In the words of Sabri Zain observations states as follows:

*It is a telling reflection of Malaysia's biggest political crisis in more than a decade. The local media generally have tended to reflect the government's viewpoint in reporting Datuk Seri Anwar's sacking, arrest and trial. Now they are coming up against critics armed with computers in the tussle to shape public opinion. Ironically, the amazing success of the Internet as an alternative voice is probably due largely to the mainstream media. Opinions that are critical of the government and the ruling political parties are given little, if any, coverage in local newspapers and television stations. The constant fear of losing their publishing or broadcasting licenses hangs like a sword of Damocles over their heads every year when they have to renew them. But Malaysians have long been used to a cowed, docile media. What probably 'turned over' most people was the way the local media went into a veritable feeding frenzy of graphic reports about the depraved sodomite Anwar, the bloodthirsty Reformists and their evil foreign backers. (Sabri Zain 6 Ogos 99, ALIRAN)*

This has indirectly revealed to us that the development of technology in the information dissemination system has given birth to a new form of power in the social life of Malaysian society, vis-a-vis, cyber power. This emerging cyber power has the same features and strengths as any other form of conventional power. Cyber power has the possession element. And this element is in line with the concept of power once conceived by German sociologist Max Weber who described the concept of power as:

*In general, we understand by 'power' the chance of a man or of a number of men to realize their own will in the action' (Weber, 1952: 180; 1986: 29)*

In view of the context of the above discussion, it is clear to us that the element of dominance is reflected in the growing cyber power. This development seems to be affecting not only physical aspects, such as the ownership of information technology tools in society, but also the dominance of the values and forms of thinking of society itself. What is interesting is that the development of value and thought by the cyber powers is colliding and undermines the influence of governmental powers that have long dominated and controlled the development of socio-political values of the Malaysian community themselves.

This emerging cyber power also has elements of social order. In other words, social rules that have been shaped by governments over the years have begun to be regulated by cyber powers. Although this cyber power exists in virtual form, it is interesting that it still creates a form of virtual social interaction among the people with discussions surrounding its new and more democratic social rules. This can be seen by looking at the socio-political issues that are discussed on most of the internet sites available on the internet. Almost 90 per

---

cent of the social issues discussed on the website are social issues of knowledge, individual responsibility and community in the context of the Malaysian democracy system. Such social issues, however, are indirectly linked to the pre-mordial social issues that have colored and shaped political development in Malaysia, particularly in the context of political alliances, policy-making and political stability. This development has directly re-educated the thinking and norms of the Malaysian community on the issue of national and community life beyond the boundaries and contexts of thinking of a particular race or group. Conceptually, these developments (cyber power & social order) coincide with the definition of the concept of power ever touched by British sociologist Barry Barnes:

*Any specific distribution of knowledge confers a generalised capacity for action upon those individuals who carry and constitute it, and that capacity for action is their social power, the power of the society they constitute by bearing and sharing the knowledge in question. Social power is the added capacity for action that accrues to individuals through their constituting a dsitribution of knowledge and therby a society. (Barnes, 1988: 56-7)*

The concept of power described by Barnes is developing in the context of the development of information technology in Malaysia. Although the dissemination of such information, as already described in virtual form, the fact that the power of cybersecurity to emerge as a social power of organizing and disseminating knowledge and subsequently expressed through daily social behavior, is interesting to consider in the context of socio-political development in Malaysia especially the democratic system. What is interesting to examine and analyze from the development of information technology and cyber power is from the standpoint of political stability and security in the context of the Malaysian democratic system. For the past six decades the most widely discussed aspect of democracy in Malaysia has been the limited and controlled space of democracy (civil society and political participation) and the dominance of governments in the management of its democratic polity. The reciprocal relationship analysis between limited democratic space and governmental dominance, has led many Malaysian political scholars to classify the Malaysian democracy system in various forms and properties, such as *Democratic and Authoritarian* (Crouch, 1996), *Semi-Democracy* (Case, 1993), *Statist-Democracy* (Jesudason, 1995), *Quasi-Democracy* (Zakaria Hj Ahmad, 1989). In the context of such a democratic system it is difficult to say that the expansion of democracy space exists. This has been explained as the government has taken control of the space through legal control and education system.

In other words, the democratic space allowed is space (either physical or non-physical) under the influence of the government. That is why, for the last 6 decades, civil society has been unable to break free from the influence and domination of the government's

---

intellectual property. Civil society that exists in a limited space of democracy is unable to carry out a process of cultural revolution among the people. This is in line with Antonio Gramsci's (1920) notion that a society's failure to compete with government hegemony is closely linked to the society's inability to conduct a cultural revolution based on intellectual freedom independent of government intellectual hegemony.

Thus, in this context the emergence of IT has directly acted as a "tool" for the weak to position themselves with the government in an arena that is no longer a hidden transcript as Scott stated in his study of the Peasant community in the state of Kedah. IT, as a form of modernization in Malaysia, has fostered the process of democratizing information in Malaysia. The emergence of the Internet, blogs and YouTube sites, for example, has dramatically increased access and transparency of information that is alternative to the government media. For example, on the eve of the 2008, 2013 and recent 2018 general election, it was reported that the *Malaysiakini*, *Malaysia Today*, *Malaysia Insight*, *SakMongkol* (to mention a few) and many others website was crashed due to the inability of the site to handle such high traffic and traffic. Also reported during the 2018 PRU14 (14 General Election) election campaign, the Malaysia Today website, run by Raja Petra, is a site that has been consistently reached by alternative media visitors. On the other hand, YouTube has been used not only as a competition arena, but thousands of people have used it to watch political talks and campaigns organized by opposition parties that they cannot physically attend.

It is clear to us that the presence of IT, especially the internet has not only enabled the democratization of information in the development of Malaysian politics, but also raised the political power of the weak to position themselves with the government at the open system. Bloggers who appear on certain internet blogs openly cast their opinions on the state of the country which they viewed as contrary to democratic norms. For example, over the past three decade, bloggers such as *Sang Kelembai*, *Kadir Jasin Blog*, *Tinta Merah*, *Shahbudin Blog*, *Ruhanie Ahmad Blog*, *Rocky'Bru* and many others, were all "daringly" expressed their opposition to governmental behavior that was not in line with democratic culture.

In addition, the contribution of WI-FI in the process of democratization of information is without doubt undeniable. WI-FI or wireless broadband has emerged as one of the "cultural traits" in today's social life style of any society and country. WI-FI has shaped a new culture or lifestyle among the people or the young generation in their access to information and their social interaction style. At locations such as Star-Bug, McDonald's, A&W, Secret-Recipe; paired with their own laptops, this STAR-BUG community expresses their world views on any issue or social issue without any political fears or governmental constraints. In other words, it can be said here that the emergence of IT within the Malaysia

socio-political structure has directly democratized and consolidated their political will. The development was also acknowledged by the former Malaysian Information Minister, Ahmed Shaberry Check, who clearly stated that the bloggers community was one of the segments of society that challenged Barisan Nasional's political hegemony in the last general election of 2018. His statement revealed that alternative media is one of the new political forces that needs serious attention today. This has indirectly informed us that technological advances, especially in the field of information dissemination, have created a new form of power in the social life of Malaysian society, vis-a-vis, cyber power.

The above discussion clearly shows us that the emergence of IT and the Internet has presented new challenges to the patterns of national and urban life Malaysian society as a whole. Malaysia as a free country for more than 6 decades has achieved a remarkable level of political, economic and social stability compared to other developing countries. In these context, it does not mean that Malaysia does not face any challenges that could jeopardize its existing and stability, nevertheless the emergence of IT and the Internet has made the challenges to the integrity of Malaysian nations are becoming more complex than ever before.

## CONCLUSION

In modern times, the reliance and widespread use of IT and the Internet has created a new form of threat to the security of a nation. We have briefly discussed above, how organizations like *Abu-Sayaff*, Al-Qaeda, and many others terrorists groups have used and adapted IT for the purpose of their struggle and attacked the said target. Malaysia is no exception in this context. In fact, recent developments indicate that Malaysia's cyber security is also exposed to security threats, whether domestic or international. Thus, the rapid growth of the cyber world requires the rethinking of not only the concept of security and its challenges, but also an increasing demands for every nation to strengthen its knowledge pertaining to cyber-world.

## REFERENCE

- Arquilla, John J & David F Ronfeldt. (2016). *Cyberwar and Netwar: New Modes, Old Concepts of Conflict*. RAND Corporation 1993 atas talian <http://www.rand.org/publications/randreview/issues/RRR.fall95.cyer/cyberwar.html>.
- Asmarani, Devi. (2017). *Jakarta-KL Dispute Sparks Cyber War-Hackers From The Two Countries Deface Nearly 100 Websites*. Malaysia Today, atas talian <http://www.malaysia-today.net/Blog-e/2005/03/jakarta-kl-dispute-sparks-cyber-war.htm>.

- Auerbach, Jon G. & William H. Bulkeley. 2000. *Web In Modern Age Is Arena For Activism, Terrorism & War*. Wall Street Journal: New York.
- Barlow, John P. (2006). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. <http://homes.eff.org/~barlow/Declaration-Final.html>.
- Barnes, J.P. (1988). *The Nature of Power*. Cambridge: Polity
- Brookes, Peter. (2005). *The Art of Cyberwar*. The Heritage Foundation. <http://www.heritage.org>.
- Delio, Michelle. (2017). *Hacktivism and how It Got There*. Wired News. <http://www.wired.com/news/infostructure.html>.
- Denning, Dorothy. (2015). Cyberwarriors: Activist and Terrorist Turn to Cyberspace. *Harvard International Review*, 23[2] pp: 70-85.
- Ho, Peng Kee. (2006). *Governmentware Seminar*. <http://mha.gov.sg/mha/detailed/html>.
- Hoffman, Bruce. (2006). *The Use of the Internet by Islamic Extremists*. RAND Corporation <http://www.rand.org/publications/randreview/issues/cyberwar.html>.
- Case, W. (1993). Malaysia: semi-democracy in withstanding the pressures for regime change. *Pacific Affairs*. 66(2): 183-205.
- Crouch, H. (1993). Malaysia: neither authoritarian nor democratic. Dlm. Hewison, K., Robinson, R. & Rodan, G. *Southeast Asia in the 1990s: authoritarianism and democracy*, hlm. 135-157. Sydney: Allen and Unwin.
- Jesudason, J. V. (1995). Statist democracy and the limits to civil society in Malaysia. *Journal of Commonwealth and Comparative Politics*. 33(3): 335-356.
- Saravanamuttu, J. (1999). Thinking the thinkable: politics after Mahathir (part 1-3). *Aliran Online*. Oct./Nov.
- Weber, M. (1952). Class, Status, Party, from Gerth, H & C. Wrights Mills (eds) From Max Weber. London: Routledge.
- \_\_\_\_\_. (1986). Domination by Economic Power and by Authority, in Lukes, S (ed) Power: readings in social and political theory. Oxford: Blackwell
- Zakaria Ahmad. (1989). Malaysia: quasi democracy in a divided society. Dlm. Diamond, L., Linz, J.J. & Lipset, M. S. (pnyt.) *Democracy in developing countries: Asia*. Jil. 3, hlm. 347-382. Boulder, Colorado: Lynne Rienner.
- Aliran Monthly, (1999).
- Asian World Street Journal, (1999).