PENDAHULUAN

Kebanyakan formasi mekanis di dunia dibantu oleh Rejimen Artileri Gerak Sendiri (*self propelled - SP*) untuk memberi bantuan tembakan dalam setiap fasa operasi yang dilaksanakan. Penggunaan meriam jenis tarik (*towed*) akan menghadkan kemampuan bantuan tembakan disebabkan oleh limitasi dan mobiliti meriam jenis *towed*. Berdasarkan perkembangan semasa, perolehan sistem meriam 155 mm SP telah menjadi satu keperluan.

Meriam SP adalah satu sistem meriam yang boleh bergerak sendiri tanpa bantuan kenderaan penarik meriam. Meriam diletakkan di atas *chasis* kenderaan samada beroda (*wheel*) atau berantai (*track*) dan pada kebiasaannya badan kenderaan adalah dari jenis *armoured* atau *hard skin*[1]. Sistem artileri terbaik untuk menyokong sesebuah formasi Mekanis mestilah sekurang-kurangnya dari jenis meriam medium 155 mm yang mana dengan kaliber dan diameter larasnya yang besar berupaya menembak peluru 155 mm ke sasaran yang lebih jauh serta mampu menghasilkan serpihan yang boleh menembusi dinding berperisai pada kenderaan Mekanis musuh.

CIRI-CIRI MERIAM SP

Keperluan sistem meriam 155mm SP adalah merujuk kepada ciri-ciri (*characteristic*) yang ada pada sebuah Bn/Bgd Mek. Antara ciri-ciri Batalion Mek adalah seperti berikut:

a. Mobiliti.
b. Komunikasi.
c. Fleksibiliti.
d. Kuasa Tembakan.
e. Perlindungan.

Berdasarkan ciri-ciri pasukan Mekanis yang digariskan, secara logiknya untuk menentukan tembakan artileri dapat diberikan sebilang masa, adalah perlu untuk pasukan artileri yang membantu formasi Mekanis ini juga mempunyai ciri-ciri yang

1. http://en.wikipedia.org/wiki/Mechanised_artillery.

setanding. Sistem meriam 105 mm jenis *towed* yang ada ketika ini didapati tidak mampu memenuhi keperluan ini. Meriam SP perlu mempunyai ciri - ciri yang sama dengan pasukan mekanis. Antara ciri-ciri penting pada sesebuah meriam SP adalah seperti berikut:

a. **Mobiliti**. Keupayaan meriam yang terletak di atas *chasis* kenderaan menjadikannya sentiasa dapat bergerak pantas dalam mengekalkan jarak tembakan. Corak deploimen secara 'rapid' dapat diikuti dengan mudah tanpa menjejaskan bantuan tembakan yang diberikan. Banyak masa dan tenaga anggota dapat dijimatkan berbanding sistem jenis *towed.*

b. **Kepantasan Bertindak**. Keadaan meriam yang telah sedia terpasang 'fitted' kepada *chassis*, memberi kepantasan masa tindak. Ini menjimatkan masa untuk anggota meriam dalam menyediakan meriam untuk menembak. Kepantasan ini juga dapat dicapai oleh kerana Meriam SP turut dilengkapi dengan sistem ukur yang membolehkan setiap unit meriam memperoleh orentasi dan fiksasinya sendiri. Sistem *Inertial Navigation System* (INS) dan *Global Positioning System* (GPS) dapat menghalakan laras meriam ke sasaran dengan cepat, dan pada ketepatan yang tinggi. Keupayaan bergerak dengan cepat untuk masuk dan keluar tindak menjadikan meriam SP boleh bertindak dengan pantas. Kebolehan tembak dan pergi atau *shoot* and *scoot* meriam SP merupakan ciri terpenting yang akan memberi kelebihan taktikal kepada formasi yang dibantu.

c. **Kaliber**. Kaliber yang besar dengan peluru 155mm menjadikan sistem meriam SP mempunyai keupayaan yang setanding dengan meriam 155mm jenis *towed*. Kaliber yang besar membolehkan peluru yang ditembak dapat membawa kuantiti bahan peledak yang lebih banyak dan seterusnya memberi kesan yang lebih besar di kawasan impak.

d. **Perlindungan**. Sistem meriam SP lazimnya mempunyai *chasis* dan badan kenderaan yang mampu memberi perlindungan kepada krew dan sistem dari tembakan senjata kecil dan senjata bantuan. Perlindungan ini memberi impak positif terhadap kemampuan seluruh bateri atau rejimen SP semasa melaksanakan aturgerak serta semasa melaksanakan pertahanan tempatan di kawasan aturduduk.

e. **Komunikasi**. Setiap unit meriam atau keseluruhan sistem SP (bateri atau rejimen) dilengkapi dengan radio HF dan VHF. Sistem komunikasi ini juga mampu menyalurkan data seperti data ukur, kajicuaca dan balistik dari kenderaan Pos Perintah terus kepada setiap unit meriam SP. Selain itu dengan sistem komunikasi tersebut membolehkan bateri/rejimen meriam SP dapat berhubung dengan pasukan yang berada jauh di hadapan bagi menjamin bantuan tembakan.

f. **Keupayaan Membawa Peluru**. Saiz kenderaan meriam SP yang lebih besar meningkatkan kecekapan dan keupayaannya membawa peluru. Pelbagai jenis

peluru dengan bilangan yang lebih banyak boleh dibawa seterusnya akan mengurangkan proses ulang bekal dan mempertingkatkan *survivability* meriam. Tambahan juga, sistem ini lazimnya didatangkan bersama dengan kenderaan pembawa peluru untuk memastikan bekalan peluru sentiasa berterusan.

PERBANDINGAN SISTEM BERODA DAN BERANTAI

Sistem meriam SP di pasaran dunia ketika ini terdiri dari jenis berantai dan beroda. Justeru satu perkara yang penting dan perlu dikaji sebelum perolehan dibuat agar sistem tersebut bersesuaian mengikut keperluan dan persekitaran negara.

Setiap sistem mempunyai kelebihan dan kekurangan masing - masing. Oleh itu bagi kawasan yang mempunyai jaringan jalanraya yang cekap di bandar dan di desa menjadikan sistem meriam jenis beroda mungkin menjadi pilihan. Namun begitu, bagi sebahagian kawasan, terutamanya kawasan yang mempunyai tanah yang tidak sekata (off road), sistem meriam jenis berantai adalah lebih difikirkan sesuai.

Walaubagaimanapun faktor lain juga perlu diambil kira dalam membuat perbandingan antara kedua-dua jenis sistem ini. Ianya dilihat dari 6 faktor berikut:

a. Mobiliti.
b. Penjimatan Minyak/Jarak.
c. *Survivability.*
d. Senggaraan.
e. *Vulnerability.*
f. Halangan dan Daya Gerak.

SISTEM BERODA

Mobiliti. Ia Mampu melepasi halangan dengan mudah dan bergerak 50% lebih laju dari sistem berantai[2]. Ia juga boleh digerakkan ke mana-mana destinasi tanpa memerlukan bantuan low loader.

Penjimatan Minyak. Berdasarkan kepada kajian oleh *US Army Materiel System Analysis (AMSAA)/ Defence Evaluation and Research Agency (DERA)* menggunakan NATO *Reference Mobility Model (NRMM)*[3] sebagai rujukan analatikal keupayaan kenderaan yang digerakkan pada jarak dan jumlah minyak tertentu, mendapati bahawa kenderaan beroda lebih efisyen dari segi penggunaan minyak berbanding kenderaan berantai pada tiga keadaan jalan iaitu jalan luar bandar, jalan sekunder dan jalan primer. Ia juga mampu menjangkau jarak operasi antara 600km ke 700km.

Survivability. *Survivability* sistem beroda tidak sehebat sistem berantai. Ini kerana, keupayaan roda untuk melepasi halangan adalah lebih rendah. Selain itu, berat kenderaan yang tertumpu pada 4 titik sentuh tayar dengan tanah menyebabkan sistem beroda mudah tenggelam atas tanah yang lembut. Walau bagaimanapun kemajuan teknologi yang terdapat pada kenderaan beroda 6 x 6 dan 8 x 8 telah berjaya mengatasi masalah ini.

Senggaraan. Sistem beroda lebih murah dan senang untuk disenggarakan serta memerlukan sokongan logistik yang lebih kecil terutama dari penggunaan jentera dan tool. Selain itu, infrastruktur khusus tidak perlu diwujudkan untuk menampung keperluan simpanan dan senggaraan sistem beroda kerana keperluannya hampir sama dengan kenderaan beroda yang lain.

---

2. Tank-automotive & Armaments Command (TACOM), 2000.

3. Self Propelled Howitzer – Tracked Versus Wheeled

Vulnerability. Tayar kenderaan beroda tidak dilindungi oleh plat-plat perisai. Walau bagaimanapun menerusi kemajuan teknologi menjadikan tayar kenderaan beroda (run flats tires) mampu bertahan terhadap letupan *improvise explosive devices* (IED) walaupun tayarnya hampir musnah[4].

Halangan dan Daya Gerak. Menghadapi sedikit kesukaran untuk melepasi halangan seperti tembok dan lain-lain. Walau bagaimanapun seperti juga faktor *survivability*, teknologi 6 x 6 atau 8 x 8 masa kini menjadikan halangan bukan lagi masalah besar kepada kenderaan beroda.

SISTEM BERANTAI

Mobiliti. Dapat bergerak lancar atas jalan tidak rata (*off road*). Sistem *Skid steering mechanism* membolehkan mudah dikemudi dan boleh mengubah arah dari 180° hingga 360°. Mampu melepasi parit dan halangan lain, walaubagaimanapun ia bergerak lebih perlahan di atas jalan bertar berbanding kenderaan beroda serta memerlukan kenderaan *low loader* untuk menggerakkannya bagi jarak yang jauh.

Penjimatan Minyak. Kenderaan berantai menggunakan minyak yang lebih tinggi kerana nisbah beratnya yang perlu ditanggung oleh enjin serta jarak operasi yang lebih dekat iaitu antara 400km ke 500km.

Survivability. Rekabentuknya lebih padat berbanding kenderaan beroda disebabkan adanya sistem seperti *advance suspension clearance dan wheel turning clearance*. Selain itu, dengan ketiadaan *multiple transfer cases* dan *drive shafts* membolehkan kenderaan berantai mampu bergerak dengan lebih lancar ketika berhadapan dengan halangan tanah. Selain itu kenderaan berantai mampu mengagihkan berat

---

4. Ibid m/s 18.

keseluruhannya pada kadar purata yang sama ke tanah menerusi lebar dan panjang *track*.

Senggaraan. Kos senggaraan untuk sistem berantai lebih mahal dan rumit. Sebagai contoh adalah untuk menyelenggara band dan *steel track* memerlukan perbelanjaan kewangan yang agak tinggi. Perolehan sistem berantai juga memerlukan infrastruktur dan kemudahan khusus seperti *hard standing* dan kemudahan penyelenggaraan yang lebih berbanding sistem beroda.

Vulnerability. Kebiasaannya badan kenderaan berantai direka supaya mampu menahan tembakan dari senjata kecil dan senjata bantuan.

Halangan dan Daya Gerak. Sistem berantai lebih berupaya merentas halangan dan mampu bergerak lancar pada semua bentuk permukaan jalan termasuk jalan tidak berturap serta mampu mengharungi gradient slope hingga 60% dan side slope hingga 30%.

KESIMPULAN

Berdasarkan pemerhatian yang dibuat berkenaan kemampuan dan keupayaan sistem meriam SP ini, dapat disimpulkan bahawa sistem ini dapat mempertingkatkan keupayaan artileri dalam memberi bantuan tembakan kepada pasukan yang dibantu seiring dengan kemajuan teknologi masa kini. Perbincangan tentang kesesuaian samada sistem meriam SP beroda atau berantai untuk membantu formasi Mek perlu pertimbangan yang amat terperinci. Sekalipun memang tidak dapat dinafikan bahawa mobiliti menjadi aspek paling penting dalam perolehan meriam SP, namun keperluan ini perlu dilihat bersama aplikasi *effect based operation* yang diamalkan di dalam sesuatu operasi artileri. Unit artileri yang membantu formasi Mekanis tidak semestinya mengikuti rapat serta melalui semua keadaan mukabumi yang dilalui oleh formasi Mekanis, kerana peranan utama pasukan artileri bukan untuk menduduki dan menawan kawasan, sebaliknya lebih kepada menentukan bantuan tembakan diterima oleh formasi dibantu. Tambahan lagi dengan kebolehan keluar dan masuk tindak dengan pantas serta daya mobiliti yang tinggi dan juga jarak jangkauan meriam 155mm yang lebih jauh, keupayaan untuk memberi bantuan tembakan sesuatu unit artileri SP adalah hampir seimbang samada ianya beroda atau berantai.

Mej Hizamuddin bin Haris telah di tauliahkan dalam Rejimen Artileri Diraja pada 18 Jun 1994 dan telah menghadiri Kursus Defence Sevices Command and Staf College pada 2009 di Mirpur, Bangladesh. Sepanjang perkhidmatan dalam Angkatan Tentera Malaysia, Beliau telah berkhidmat di Rejimen Pertama Artileri Diraja (Para), Pusat Latihan dan Markas Tentera Darat. Antara jawatan yang pernah disandang adalah Ketua Seksyen, Ketua Terup, Jurulatih Cawangan Pengesan, Ketua Bateri, Penolong Pegawai Memerintah dan Timbalan Komandan. Beliau juga pernah bertugas di bahagian *Joint Fire Wings* (JFW) melalui Malaysia Australia *Joint Defence Program* (MAJDP) sebagai Jurulatih Guneri yang ke-10 di School of Arillery, Puckapunyal, Victoria, Australia dan penguji di School of Armour, Puckapunyal, Victoria, Australia bagi kursus yang memerlukan nasihat dan kepakaran artileri.

FREEDOM OF INFORMATION, THREAT TO NATIONAL SECURITY

by Maj Azwan bin Abdul Aziz

Right to know and access on government information or in another word, Freedom of Information (FOI) by public is very crucial in today democracy society. It can be define as *"an extension of freedom of speech, a fundamental human right recognized in international law, which is today understood more generally as freedom of expression in any medium, be it orally, in writing, print, through the internet or through art forms"* (Arnold, 2005).

FOI is part from the Freedom of Expression fundamental under the Article 19 of the Universal Declaration on Human Rights (UDHR) where people has the right to the knowledge through any media without any barriers (Mendel, 2003). This fundamental is accepted globally and widely agreed that a democratic political system requires adequate and effective level of public information (Melanson, 2001).

It is also agreed that FOI is a basic principle and an indicator for a democratic country. When a government is transparent, it will help fight the corruption and promote more accountability (Silva, 2010). That why FOI is becoming standard good practice in the international community. On the current situation, FOI has been adopted by over 95 countries around the world where the first FOI law implemented by Sweden in 1766 which is over 248 years ago (Silva, 2010). The vast development of internet technology simplifies the public to seek information and make the public start to realize, understand and took care of their right more seriously and more concern on government matters.

To fulfil the basic right of the public to know of FOI fundamental, government are required to be transparent and provide access for the public on information held by government agencies. Generally, information held by the government agencies should be access by the public and Article 19 of UDHR strengthen this statement. Under the FOIA, public right to seek, receive and impart all information regardless of frontier including military, defence, economy, political and social matters. Due to this requirement and need for openness country, FOI seem a threat to national security that can affect the national sovereignty, integrity and security of the country. It is an ongoing battle between secret keepers and those seeking access; between those who value national security or privacy more than a public right to know and those who hold the opposite position; between agencies seeking to shield themselves from the burdens and consequences of the disclosure process and citizens who demand greater accountability (Melanson, Secrecy Wars-National Security, Privacy, and the Public's Right to Know, 2001). For this reason, there are possibilities for the FOI to be sacrificed in exchange for secrecy of national security. Due to this problem, this paper is to discuss although the

FOI is a threat to national security and how to reconcile it without compromise the right of the public.

In Malaysian context, Malaysia had restricted access to FOI (Anynamous, 2013). Under ruling party Barisan Nasional (BN) coalition, Malaysia had imposed several laws such as The Sedition Act and harsh criminal defamation laws to restrict the press and public from criticise the government although the constitution guarantees the FOI under Article 10. Put on jail are among the punishment for who that violate these laws. In 2011, the states that been controlled by the opposition party such as Selangor, Penang and Kelantan had passed the FOI laws, however as a whole, Malaysia still don't have federal law relating to FOI and government agencies still refuse to share documents. Official Secrets Act (OSA) also threaten government servant in Malaysia.

As an example, Syed Abdullah Hussein al-Attas; a blogger had been detained in prison under OSA after posting a controversial statement on Sultan of Johor. Although his statement support with documents claiming that he had the right from the fortune left by late Sultan Iskandar and some report said that, that document also disappeared (Anynamous, 2013).

Malaysia had face the vast development of information technology and the internet nowadays, with the rate of the accessing internet increasing to 66% of population in 2012. Malaysia had imposed of refraining policy for direct online censorship, under the Section 3(3) of the Communication and Multimedia Act (CMA) and the Multimedia of Guarantees (Anynamous, 2013). Restriction on press had caused the increasing of online news and blogs that offer a different point of view. Although these blogs are independent. However may suspect had affiliate with politician either to the ruling party or opposition that offer different opinion and view that cannot be find in the traditional media. Whistle-blower in Malaysia also takes this opportunity to fight the corruption and human right abuse.

As the world is moving forwards towards pure democracy, citizens are more demanding on nowledge's and information's on all government matters and government are required to be transparent. It gives a check and balance, public participation in government matters and safeguards against abuses power. As in theory, the government should give the public free access on government information because government are the servant to the public. This will contribute to a good government and towards a better world. As the enforcement of FOIA, it ensures this objective can be achieved and abide by all.

However, the protection of national security and its citizen also important.What is the effect of FOI to the national security? It is possible for the citizens to get information on military secret information's, government to government negotiations or future economic planning. How about an act of whistle-blower such as WikiLeaks who discloses wrong doings in the public interest? Chapter Three as the main chapter will discuss and

analyse of FOI and its effects towards National Security. The pros and cons will be discussed thoroughly and also issues relating to three aspects which are military, political and societal.

On the other hand, inmilitary, most of the information's are been classified to secret and highly sensitive towards national security that some of this information need protection for some duration years. Information such as critical base locations, level of readiness and secret operations are very sensitive and must be veryprotected in order to conduct military and intelligence effectively. Confidential information can be used by the enemy against the country and this will involve casualties and death.After the War on Terror been launch on 2011, FOI frequently been compromised and limit in the name of national security (Tejera, 2013). This war includes many features of information battles on many fronts such as scientific and technical, presidential report, online censorship and public safety information (Mendel, 2003).

In the past, information's relating to military operations are kept confidential for a certain period because it involves military warfare tactics and techniques of the country. What is more important and concern for the public to know is the result of the operation is either successful or otherwise. But this has changed. With the proliferation of information technology and the pressure from FOIA requirements, information's on military operations are needed by public and easily access such as on the internet whether the information provided by agencies are recognized or not such as information leaked by WikiLeaks.

Information through sources that are recognized such as from Ministry of Defence Portal is always had an objective on assisting government in winning the hearts of the people. Activities such as participation in UN missions, disaster relief and military activities with public is most-highlighted. Other activities are limited due to factors of confidentiality. No one knew what and how the military doing their business. However, the vast development of information technology has changed this. WikiLeaks, for example, has revealed the Afghan War Diary in July 2010, a compilation of more than 76,900 documents containing relevant documents in Afghanistan war that were not previously available to the general public. These documents have revealed a number of deaths involving civilians by the military which keep in secret by US military (Karhula, 2012). Later in October 2010, WikiLeaks once again revealed a total of 400,000 documents called the Iraq War Logs to the main mass media. The "war logs" is an evidence how human right been abuse by the US towards civilian (Karhula, 2012).

Through a military perspective, the information that was leaked had undermined the efforts to combat global war on terror (Karhula, 2012). Besides revealing information on how military operate, the leaking also revealed to the public the crucial targets, objectives and intelligence sources, whether individual or allied countries. Due to the lots of confidential information's been known by public, therefore, the military should restructure or find other methods in conducting their mission, objectives and also to save soldier life.

But this opinion is different from public view. Success is not the only consideration on how the mission will be conduct. At this point, peoples are more sensitive to the offenses committed even during the war. Persecution and death of civilians must be defended. Although it was difficult to get information from the military, the information obtained from the Internet is faster and practical. Therefore, the military should be more careful with the mission done.

In the present war, information is paramount and importance in determining the survival of the country and the success in a mission or a war. As an example, war on terror had showed us how countries in the world involves in gathering sensitive information about terrorist at home or abroad. Therefore, it cannot not be denied that most of the countries especially who involve in the conflict are conducting activities of gathering information and monitoring by intelligence agencies from time to time. Intelligence activities and information's obtained are highly secret because it involves the safety of intelligence and sensitive issues on other country. Leaking of this information will involve the security of intelligence personnel and relationship to the country will be affected. So how to decide, which information should public know and which must be protected.

For example, in year 2013, WikiLeaks has been displaying a secret document on the Internet about Australia that conduct intelligence activity on president of Indonesia. The secret document revealed theactivities of tapping on cell phone of President Susilo BambangYudhoyono, his wife Christian Herawati and another eight government Ministers and Officials in 2009 (McGuirk, 2013). As a result of the WikiLeaks report, Indonesia president has called back his ambassador to Australia immediately and asking the ministry of foreign affairs to review bilateral cooperation. Indonesian ambassador to Australia had said and gave warning to the press that Australia should not under estimates Indonesia tolerance (McGuirk, 2013). On the other hand, Australian Government decline to comment on the report and his Prime Minister had issued a statement that gathering information is what every government should do and it is a fact. The Australian government uses all the resources of this intelligence in order to help and support the allies and friends (McGuirk, 2013).

Besides Indonesia, reports that had been disclosed by WikiLeaks also affected the good relations between Malaysia and Singapore. The report disclosed by the Dutch media NRC Handelsblad have said about the "Stateroom Programme" which involves intelligence cooperation between five countries, namely USA, UK, Australia, Canada and New Zealand, or better known as "five eyes". Dutch newspaper NRC Handelsblad source revealed Singapore Intelligence Department (SID) by using Singapore Telco SingTel had spying through communication cable SEA-ME-WE-3 which connecting Southeast Asia region, Middle East and Western Europe to communicate either by phone or internet (Hassan, 2013).

The Malaysian government has sought an explanation, however been denied by Singapore government. As the Deputy Prime Minister said "If it proved true the

Singapore spying through cable SEA-ME-WE-3 is quite sure these events could have an impact on diplomatic relations because the communication channel is not only used for international communication, but also for use in the state. Too much confidential information which should not be known as the Singapore issues of water price negotiations, overlapping claims BatuPuteh, Middle Rocks or South Escarpment, the status of land belonging to the Malayan Railway, Malaysia's intention to replace the causeway with a bridge or disputes about Singapore's actions to implement the reclamation at Straits of Johor" (Hassan, 2013).

In military aspect, locations of key installations such as the missile defence systems, radars and airfields are a strategic and tactical asset that needs to be protected from the enemy. If this information falls to the enemy, it could jeopardize the safety not only to that installation but also to the safety of the country.

At this point, most of the political parties in many countries are more likely to make efforts to make the administration and conduct of the government more transparent. US government under President Obama administration had ordered all government agencies to be more transparent as he said in a memorandum of Transparency and Open Government. "Government should be transparent because transparency will encourage accountability and feed the citizens with information on what their government is busy on to. Information withheld by the government agencies must be protected as national assets. My administration will take appropriate action, to assure the FOI can be access by the public consistence with FOIA and policy" (J.Piotrowski, 2010). Somehow national security has been misappropriated to hide illegal arms sales, drug trafficking, and covert operation meanwhile secrecy has been distorted by agencies such as FBI to hide it surveillance of political leader and celebrities whose right to privacy (Melanson, Secrecy Wars-National Security, Privacy, and the Public's Right to Know, 2001). As in Malaysia, a popular online paper, Malaysiakini was raided by Malaysian Police on 20 Jun 2003 for breach under sedition act after publishing a letter relating to national policies in favour of ethnic Malays by comparison to the US that on the basis could cause racial disharmony (Mendel, 2003).

FOI is seen as a way to create a better government and harmony citizens with effective of government bodies. The decisions of the government are more to meet the goals and fulfil people requirement. The knowledge that decisions and process are open to scrutiny, including under the FOIA, impose a constant discipline on the public sector (Banisar, 2006). For example, the FOI is now used as a tool to fight corruption when all the documents such as contract dealings and financial transactions should be made and kept in complete and can be accessed by the public. There is a case in India where an activist group has used FOIA to obtain information on government development projects. This activist group has uncovered flaws on projects where payments are not recorded correctly or not accurate (Banisar, 2006). In a bigger scandal which was UK Members or parliament expense scandal in 2009. Members of Parliament has sought to obtain parliament members expense in relating to the UK FOIA. Although it was initially

difficult to get information and should appeal through the tribunal, finally a complete set of documents been obtained and manipulation and fraud such as mortgage payment among the members of parliament. This exposure has resulted in major changes to the members of parliament including resignation (Banisar, 2006).

FOI is a powerful tool in promoting public for Participation in the planning of activities, decisions and policies of the government. The public could contribute and participate effectively in country matter if they had enough information and knowledge (Banisar, 2006). Increased participation of the public will enhance administrative efficiency and improve the quality of thedecision. Public servant are benefited to the knowledge by accessing to the knowledge that been spread widely in the society (J.Piotrowski, 2010).

FOI can improve many of the societal rights and security. One case in Thailand where a mother was complaining why his daughter denied to entry elite public school. When he appealed to the Information Commission and the courts. In the end, he obtained information indicating that the children of influential people who accepted to the school even if they got a low score. As a result, the State Council issued an order that all schools accept students only on merit. In the United States, used FOIA to reveal cases of torture and illegal surveillance of government approved (Banisar, 2006).

Among the nations that make a shift to democracy, FOIA allowsthe governments to break from the past and permit the society and the victimized people and their groups to realize what had happened and feel the better of the new environment. Almost all of recent countries incorporate a right to get to data from government agencies as a human right. As an example, taking after the disintegration of the Soviet Union, most Central and Eastern European nations embraced laws to manage the access to the documents that relate the power of previous secret police. For a few nations, these records are made accessible for people to see what is constantly hung on them. In different nations, the records are constrained to "lustration" advisory groups to guarantee that people who were in the past secret administrations are denied from being in the current government or at any time their records are made open. In Mexico, President Fox in 2002 requested the declassification of every last one of records of past human rights abuse so that the families could figure out what happened to their friends and family who vanished. In the US, the National Security Archive has made a large number of request and receive data from the US government on records to identify the human rights abuse in Mexico, Peru and Chile that they make accessible to the Truth Commissions in those nations (Banisar, 2006).

As part of the government management and security matter, personal information been collect by the government and stored in the database. This data cannot be access freely by anybody due to the classification and this creates a conflict to the FOI when the public request for the data especially data of another person. This data have also been used by other agencies such as police and commercial banks. This situation violates the information privacy of individual. Generally, the FOI law provides exemption on personal

information to protect the individuals. However vary of definition and classification made the exemption hard to handle by the authorities. This can cause information such as police files and medical files leak to the other person of the organisation such as commercial agencies that had interest on personal information such as to sell it to another business agencies. It other hand, it is not possible for an individual to request their document from government bodies such as police files and intelligence files.

Meanwhile, FOI requirement also affects the Political security. Government affairs are required to be more transparent and have more participation from the public. Public are seen more powerful. Although this situation gave advantage to the public, however there are some circumstances that require secrecy and confidential that prevent or affect the stability and security of the nation. Some information need to be secret due to avoid a panic situation among public. As an example, taking consideration of the Malaysian conflict with Sulu Rebellion, some intelligence or information on Sulu desire on intervention need to be hidden from public for a period of time for government to prevent and for the safety of security forces. Leakage of this unconfirmed information to the public will create chaos and fear the public especially who live in the tension area.

As a conclusion, FOI is very important in today democracy society as a tool for check and balance. FOI encourage the public to keep knowledgeable about the actions of its government. As the world is moving toward more pure democracy, government are needed to be more transparent for less room for corruption and more room for accountability. The government servant a behave themselves because their attitude or what they do can be disclose on public. Public seem to have more power in the future. FOI is guaranteed under FOIA or other legislation that had been implemented by over 95 countries around the world. This showed us the advantage and impact of FOI towards the better world. However, the implementation of FOI is reported to be difficult due to lack of public awareness and understanding of the law on how to exercise their statutory right, confusing policy and bureaucratic on accessing information. Only advance country such as United States, Japan and UK had high level and rates of FOI request. Third country and develop country still in low level and rates of request although FOIA had been implemented for many years.

Despite from the advantages, on the other hand, FOI likely seem to threaten the national security especially when public request information relating to national security such as defence matter and secret negotiation. Unauthorized release of information can be a threat to international affair or could affect the conduct of negotiations. As been said earlier, FOI is a battle for information war on many fronts such as scientific and technical information, presidential reports, online censorship and public safety. If such tactical or ongoing mission information were released, it could put our troops in harms that involve life and death. Incident such as, leaking of information by military or intelligence personnel on war such as in Afghanistan during war on terror had showed us the possibility of the area where the FOI can cause conflict and security threat to national security.

After the terrorist attack on September 11,2001, many countries seem to amend their FOI act in order to curb terrorism act. FOI and human right seem to be suppressed and compromise in the name of national security. Statistical data had showed us that number of requests been denied for public access keep increasing each year approximately about 51.5% especially on defence matters. Other laws such as OSA has also been use by several countries to restrict the FOI and to balance between FOI and the need for national security. Several person had been accused and trial for disclose confidential document such as MI5 intelligence officers, private who disclose war log of Afghanistan or Malaysiakini that post controversial documents. This is the result from the balancing of national security with human right where in seeking to safeguard national security and community safety, the state places limits upon the exercise of human right and civil liberties (Williams, 2006).

Whistle-blower had showed the most-likely threat from the FOI towards national security. Due to a posting on the internet and without permission and filtering from the authority agencies, the information could lead into a security threat especially when dealing with security aspect. Public panic is one from the security threat where the unfiltered information can cause major damage such as ethnic disharmony especially on multiracial country such as Malaysia. Leakage of confidential documents such as military logs, intelligent report and military missions had affected relations among countries or gave bad perspective to public. Incidents such as Australia intelligence agency tapping on Indonesian leaders phone call not only affecting the relationship both countries but also affected the stability of the country in ASEAN region. However, Whistle-blower also been proven as an effective way to make the government work better in term of transparency and effective management. Due to that several country such as South Africa had imposed laws to protect a person who act as whistle-blower in the name of public interest.

As an overall, after a thorough analysis, it can be concluded that, FOI is a threat to national security especially when the information been disclose without clearance from the authority or agencies. However, FOI is important in promoting transparency and effective mechanism in combatting corruption. Due to that reason it needs for the government to balance between the requirement of FOI with the need of national security in order to take full advantage and benefit from FOI. FOI is a human right and cannot be abuse or violate.

BIBLIOGRAPHY:

1. Anynamous. (2013). Freedom House. Retrieved from Malaysia: http://www.freedomhouse.org/report/freedom-press/2013/malaysia
2. Arnold, A. P. (2005). Freedom of Expression, The Essential of Human Rights. United Publishers.
3. Banisar, D. (2006). Freedom of Information Around the World 2006, Global Survey of Access to Goverment Information Laws. Privacy International. Retrieved Jul 12, 2014, from http://www.freedominfo. org/documents/ global_survey2006.pdf
4. Barry Buzan, Ole Waever, Jaap de Wilde. (1998). Security, A New Framework for Analysis. Colorado: Lynne Reiner Publishers,Inc.
5. Birchall, J. (2013, June 12). Open Society Foundations. Retrieved from New Principles Address the Balance between National Security and the Public's Right to Know: http://www.opensocietyfoundations.org/press-releases/new-principles-address-balance-between-national-security-and-publics-right-know
6. Chirwa, B. G. (2013). National Security And The Right To Information: The Case Of Malawi. National Security And Right To Information Principles (pp. 10-12). Johannesburg RSA: University of Witwatersrand. Retrieved June 11, 2014, from https://www.google.com.my/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0CCUQFjAB&url=http%3A%2F%2Fwww.right2info.org%2Fresources%2Fpublications%2Fpretoria-finalization-meeting-april-2013-documents%2Fnational-security-and-rti-in- malawi%2Fat_
7. Frederick, S. a. (2013). Keselamatan Maklumat di dalam Penggunaan Laman Sosial Facebook di kalangan anggota tentera. Kuala Lumpur: Universiti Pertahanan nasional Malaysia.
8. Hassan, A. (2013, Nov 28). Utusan Malaysia. Retrieved Jul 13, 2014, from Singapura perlu berterus terang: http://www.utusan.com.my/utusan/Rencana/20131128/re_02/Singapura-perlu-berterus-terang
9. J.Piotrowski, S. (2010). Transperancy and Secrecy. Maryland: Lexington Books.
10. Karhula, P. (2012, Oct 5). International Federation of Library Associations and Institutions (IFLA). Retrieved from What is the effect of WikiLeaks for Freedom of Information?: http://www.ifla.org/publications/what-is-the-effect-of-wikileaks-for-freedom-of-information
11. Lundberg, K. (2011). Friend or Foe? Wikileaks and the Guardian. The Journalism School Knight Case Studies Initiative, 1.
12. Macmillan Dictionary. (n.d.). Retrieved June 9, 2014, from http://www.macmillandictionary.com/dictionary/ british/national-security
13. Macmillan Publishers. (2014). Macmillan Dictionary. Retrieved June 11, 2014, from http://www. macmillandictionary.com/dictionary/british/freedom-of-information

14 Vleugels, R. (2009, Sep 7). Overview of All 90 FOIA Countries And Territories. Fringe Special. Retrieved from http://www.cdc.gob.cl/wp-content/uploads/documentos/fringe_special_90_foias_sep_7_2009.pdf
15. Williams, B. G. (2006). Balancing National Security and Human Rights: Assessing the Legal Response of Common Law Nations to the Threat of Terrorism. Jurnal of Comparative Policy Analysis, 8(1), 48-58. Retrieved June 11, 2014, from http://www.gtcentre.unsw.edu.au/sites/gtcentre.unsw.edu.au/files/mdocs/terrorism Balancing.pdf

Mej Azwan bin Abdul Aziz earned a Diploma of Strategic Studies from National Defence University of Malaysia (NDUM) and graduated with Degree of Computer Engineering from University of Technology, Malaysia(UTM) in 2000. He joined the cadet officer training in May 1996 and was commissioned to the Royal Artillery Regiment in 2000. He has held various staff and units appointments such as Staff Officer Grade 2 Technical at Artillery Directorate and Battery Commander 31st Royal Artillery Regiment. Currently, he is the Second in Command 32nd Royal Artillery Regiment

INTRODUCTION

Today's world is becoming increasingly dependent on computers and increasingly connected through the Internet. These two facts have created a new battlefield for countries to wage war on. Using various methods of cyber attacks, depending on the situation, an aggressor country can cripple or demoralize its target without using any military force and can do so with almost total anonymity. If combined with a traditional military force, a successful cyber attack can prevent an enemy from mounting an effective defense, making the military action more likely to succeed with fewer casualties. No country has yet admitted to organizing a cyber attack, but it is likely that at least one country has successfully launched a cyber attack in such a way that it can't be proved. In the near future, cyber warfare will become more popular to antagonize other countries, but will never be used openly due to the possibility of mutually assured destruction.

Cyberwar is warfare, hostile influence which is fought in cyberspace. [1]Cyberwar is netwar by the military. It includes hackers, listeners of communications systems, van Elckradiation115 listeners and so on. Cyberwar consists of information terrorism, semantic attack, simulation warfare and Gibson warfare. Typically Cyberwar is warfare, or hostile influence between attack-and defence programs in computers, computer networks and communication systems.

For many, the term cyber war conjures up images of deadly, malicious programmes causing computer systems to freeze, weapon systems to fail, thwarting vaunted technological prowess for a bloodless conquest. This picture, in which cyber war is isolated from broader conflict, operates in an altogether different land from traditional warfare and offers a bloodless alternative to the dangers and costs of modern warfare, is attractive but unrealistic. Such a scenario is not beyond the realm of possibility, but it is unlikely. Cyber warfare will almost certainly have very real physical consequences. Computer technology differs from other military assets, however, in that it is an integral component of all other assets in modern armies. From this perspective, it is the one critical component upon which many modern militaries depend, a dependence that is not lost on potential enemies.

---

1. Cyberspace is often used as a metaphor for describing the non-physical terrain created by computer systems and also the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. See, for instance, [http://aol.pcwebopedia.com/TERM/c/cyberspace.html].

Countries around the world are developing and implementing cyber strategies designed to impact an enemy's command and control structure, logistics, transportation, early warning and other critical, military functions. In addition, nations are increasingly aware that the use of cyber strategies can be a major force multiplier and equalizer. Smaller countries that could never compete in a conventional military sense with their larger neighbours can develop a capability that gives them a strategic advantage, if properly utilized. As a RAND[2] Corporation study pointed out in the mid-1990s, the entry costs for conducting cyber war are extremely modest. Not surprisingly, therefore, countries that are not as dependent on high technology within their military establishment consider such dependence a potential "Achilles heel" for their enemies.

DEFINITION

Cyberwarfare is any virtual conflict initiated as a politically motivated attack on an enemy's computer and information systems. Waged via the Internet, these attacks disable financial and organizational systems by stealing or altering classified data to undermine networks, websites and services.

Cyberwar refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.

The fundamental weapon and target in cyber war is information. It is the commodity which has to be manipulated to the advantage of those trying to influence events. The means of achieving this are manifold. Protagonists[3] can attempt to directly alter data or to deprive competitors of access to it. The technology of information collection, storage, and dissemination can be compromised. Using other, subtler techniques, the way the data is interpreted can be changed by altering the context in which it is viewed.

This form of warfare may involve diverse technologies, notably for command and control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend-or-foe, and for "smart" weapons systems, to give but a few examples. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits.

---

2. RAND- Corporation is a research organization that develops solution to public policy challenges to help make communities throughout the world safer and more secure,healthier and more prosperous.

3. The Proceedings of the 6th International Conference on Information Warfare and Security- The Evolution of Information Assurance (IA) and Information Operations (IO) Contracts across the DoD: Growth Opportunities for Academic Research – an Update-p15-p16.

Cyberwar has broad ramifications for military organization and doctrine. Moving to networked structures may require some decentralization of command and control. But decentralization is only part of the picture: The new technology may also provide greater "topsight," a central understanding of the big picture that enhances the management of complexity. This pairing of decentralization with topsight brings the real gains. Cyberwar may also imply developing new doctrines about the kinds of forces needed, where and how to deploy them, and how to strike the enemy. How and where to position what kinds of computers, sensors, networks and databases may become as important as the question once was for the deployment of bombers and their support functions.

As an innovation in warfare, cyberwar may be to the 21st century what blitzkrieg was to the 20th century. At a minimum, cyberwar represents an extension of the traditional importance of obtaining information in war: having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the enemy before he does the same to you.

THE HISTORY OF CYBERWARFARE

From governments to major corporations, cyber attacks are growing rapidly in scope and frequency across the globe. These attacks may soon be considered an "act of war"[4] so having the latest information security training is becoming increasingly important. To be prepared for the future, you must also learn from the past.

Cyber attacks continue to grow in number and sophistication each year. In 2006, Russian Mafia group Russian Business Network (RBN) began using malware for identity theft. By 2007, RBN completely monopolized online identity theft. By September 2007, their Storm Worm was estimated to be running on roughly one million computers, sending millions of infected emails each day.

In 2008, cyber attacks moved from personal computers to government institutions. On August 27, 2008 NASA confirmed a worm had been found on laptops in the International Space Station; three months later Pentagon computers were hacked, allegedly by Russian hackers. Financial institutions were next. The State Bank of India (India''s largest bank) was attacked by hackers located in Pakistan on December 25, 2008. While no data was lost, the attack forced SBI to temporarily shut down their website and resolve the issue.

There are three main methods of cyberwarfare: sabotage, electronic espionage (stealing information from computers via viruses) and attacks on electrical power grids. The third is perhaps most alarming. The North American Electric Reliability Corporation (NERC) warned in a public notice that the U.S. electrical grid is susceptible to

4. - Lewis University's online Information Security Program - See more at: http://online.lewisu.edu/msis/resources/the-history-of-cyber-warfare#sthash.

cyberattacks, which could lead to massive power-outages, delayed military response and economic disruption.

This assumes hackers access equipment which controls the grid, something which Howard Schmidt, head of U.S. cyber security doesn't believe has happened. This development was presaged by the Cold War, but is even more obvious in the war against terrorism in the wake of the 11 September 2001 attacks on the World Trade Center and the Pentagon. It suggests that the computerized information systems of NATO member states are likely to be the continuing target of attacks by a non-traditional enemy, whose main goal is physical destruction and disruption and who is likely to exploit vulnerabilities wherever they are to be found. In this connection, it is worth emphasizing that cyber war is not the defacement of web sites owned by a rival nation, organization or political movement. Even when they accompany other tensions or hostilities — as they did during NATO's Kosovo air campaign in 1999 — such attacks on web sites are best understood as a form of harassment or graffiti and not as cyber war per se.

CURRENT WORLD AFFAIRS AND CYBER WARFARE

As with any warfare, cyber warfare can be a key issue in international politics. However, unlike traditional warfare, cyber warfare makes it difficult, if not impossible, to know who the attacker is. Even if an attack can be traced back to its origin, it doesn't mean that country was behind the attack. Because of this, there has been an arms race to get a fully operational cyber division in several countries that is prepared to either mount a cyber attack or defend against one. This is confirmed by McAfee, which reported an increase in government-based cyber warfare[5].The major world players in the cyber arena so far have been the United States, China, Russia, and North Korea.

In February of 2010, the United States launched Cyber ShockWave, a cyber war game to see how the nation would be able to respond after a serious cyber attack. The result showed that the US was not well-prepared for such an attack[6]. A number of things need to be done to get the country up to par. First, it needs to be clearly stated what powers the government has in this state of emergency. Second, there needs to be some policy in place that state how much control over the Internet and privacy the government would have. Third, a system must be developed that allows public and private security experts to work together during the attack. Finally, a policy must be drawn up that outlines how the US would respond if attacked by another nation. This would also serve as a deterrent from mounting a cyber attack on the US . Also, malware has been found in the US electrical grid that could allow the attackers who put it there to interfere with

5. [Brodkin07] Jon Brodkin. "Government-sponsored Cyberattacks on the Rise, McAfee says," Network World.http://www.networkworld.com/news/2007/112907-government-cyberattacks.html

6. [Chertoff10] Chertoff, Michael. "Cyber ShockWave Exposed Missing Links in U.S. Security," Government Computer News. p. 1, 2. March 10, 2010 http://gcn. com/Articles/2010/03/15/Commentary-Chertoff-Cyber-ShockWave.aspx

the system[7]. This suggests that attacks may already be coming or are coming soon. Some analysts report that the US is so vulnerable to cyber attack that it should be viewed a deterrent against going to war. The reasoning is that if the US tries to attack a country, it will retaliate with cyber attacks that cripple the US electricity grid, banking, or other vital services .[8]

Because US Cyber Command is part of the military, some people are worried about the militarization of the Internet. However, the US has never officially launched a cyber attack. The US did almost use cyber attacks before going into Libya[9] . Officials have said they don't want to set a precedent by being the first to openly use cyber warfare, and it's better to keep the US's capabilities secret for as long as possible. There is evidence, however, that the United States and Israel were behind the Stuxnet attack on Iran as an attempt to slow down Iran's nuclear program.

China is a perfect example of how difficult it is to say exactly who is behind a cyber attack. In December of 2009, 34 US companies were victims of cyber attacks. One of these was Google, who reported that the Gmail accounts of Chinese human rights advocates in China, Europe, and the US were hacked into. The other targeted companies happened to specialize in areas that the US is doing much better than China, suggesting that the attacks may have been to steal information[10]. Even with all of this information, it is impossible to say for sure that China is behind the attacks because it may be the case where someone is trying to antagonize China-US relations. Google was convinced China was behind the attack and threatened to pull its operations out of China. Google ended up staying in China, but this shows that a private company may have more sway that a country on the cyber battlefront.

In 2007, Estonia decided to move a Soviet World War II era monument from its capital. This was met with stiff resistance from the Russians in Estonia as well as from Russia itself. In response, Russians in Estonia began protesting. Then, Estonia became the first country to be the victim of a coordinated cyber attack. It started slowly, but ended up taking down the government websites and banking sites. The loss of banking was especially bad because about 97 percent of Estonia's banking takes place online[11].

---

7. - Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies," Wall Street Journal. p. 1. April 9, 2009.http://online.wsj.com/article/ SB123914805204099085.html

8. Baldor, Lolita C. "Cyber Weaknesses Should Deter US From Waging War," MSNBC. p. 1. November 7, 2011.http://www.msnbc.msn.com/id/45199096/ns/ technology_and_science-security/t/cyber-weaknesses-should-deter-us-wagin

9. Wagenseil, Paul. "U.S. Reportedly Considered Cyberattack on Gadhafi," Security News Daily. p. 1 October 17, 2011. http://www.securitynewsdaily.com/obama-gadhafi-cyberwar-1247/

10. -Weldon, Owen. "Google China Cyberattack Part of Vast Espionage Campaign," p. 1. January 13, 2010.http://digitaljournal.com/article/285641

11. -Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," p. 1. 2007.http://www.iar-gwu.org/node/65

This also took down Estonia's ATM system and prevented Estonians from withdrawing money outside of Estonia, as well. News and media outlets were attacked, too. Eventually, the government cut Estonia off from the rest of the Internet to stop the attacks, which allowed the country to recover and re-establish internal connections. While it appears obvious that Russia was behind the attacks, the Russian government denied all involvement, and of course it can't be proved one way or the other.

In 2008, Russia was involved in a 10 day war in Georgia. 3 days before Russia took military action, there was an attack on Georgia's networks. The government sites were either defaced or hit with a DDoS attack, news, media, and financial institutions were attacked with DDoS, and malware was uploaded onto Georgian websites. This marks the first time that a cyber attack coincided with traditional military action[12].

North Korea is in an ideal position for cyber offense. The nation itself has limited Internet access due to Kim Jon Il restricting its use, making it a weak target. However, North Korea neighbors the country with the best Internet connectivity; 95 percent of South Korea has high-speed Internet access[13]. So, if the North Koreans can connect to a computer in South Korea, from there they have a high speed connection to almost anywhere. In April of 2011, half of the servers owned by a South Korean bank crashed, and evidence pointed to North Korea. Again, North Korea denies these accusations, but most countries don't believe that. Now, there is some worry that they will escalate to South Korean military targets and get military secrets of South Korea or its allies. Some South Korean military networks had been compromised in the past, but their security has been upgraded.

Kim Heung-Kwang is a former North Korean computer science professor who defected to South Korea. Kim says that in North Korea, elementary students who excel at math are identified and prepared for cyber warfare from that early age. At the university level, they are trained at specific institutions in North Korea, and then they study in either China or Russia for additional training. This system produces around 50 new recruits every year for North Korea's cyber warfare division, Unit 121. However, this information has not been verified by another source.

INTERNATIONAL COLLABORATION

With such power and anonymity behind cyber attacks, the best way for nations to defend themselves is to work together. After the attacks on Estonia in 2007, NATO (North Atlantic Treaty Organization) decided to establish a cyber defense center. The

12. -Tikk, Eneken; Kaska, Kadri; Runnimeri, Kristel; Kert, Mari; Taliharm, Anna-Maria; Vihu, Liis. "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence. p. 7-13. November 2008. http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

13. -Harlan, Chico; Nakashima, Ellen. "Suspected North Korean Cyberattack on a Bank Raises Fears for S. Korea, Allies," Washington Post. p. 1, 2. August 20,2011.http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_ story.html

Cooperative Cyber Defence Center of Excellence was established in Estonia to research cyber warfare attacks and cyber defenses. In June of 2011, NATO established the NATO Policy on Cyber Defence. This policy contained several important parts. First, it requires that all NATO structures must be brought under centralized protection with new security rules. It also states how NATO will response to cyber threats and how NATO will assist its members if they request assistance in setting up cyber defense. Finally, the policy states how NATO will cooperate with members, international organizations, private entities, and academia[14]. The goal is to share as much information as possible and build upon it so everyone involved can be as protected as possible. Such a large scale effort to defend against cyber attacks would be difficult for a single country to fund and maintain, but a collection of countries working together can do it successfully.

DEFENSIVE CYBER WARFARE

How the concept of cyber defence could be designed? The developments policies of cyber defence are already in progress and there are basically three key elements. Firstly, deals with Security Managements and Operational Security. This consists of ensuring that there are laid down policies and procedures for the managements of our systems. In particular, the need to have some specials procedures for things such as user access, what the systems can be and cannot be used for, and what actions to take in the event of security breaches. The mechanism which allows us to the policy we have developed should be relatively forward with the military organization because we are capable of conducting and published the Information Systems Security Practice and Procedure, which can be enforced along the chain of command, just like routine orders or standing order. In addition, the need to have a mechanism in place for ensuring compliance, which basically about providing a set of procedure so that we can be assured that our soldiers are followings the rules.

Secondly, dealing with network security, there are basically three areas with which needs to concern the military organization. The first of these is the fixed network which would logically include the computers, printers, servers and other similar products which would find in the present market and commercial organization. The majority of these device will be connected to the Local Area Network (LAN) and there is nothing unusual about the required security arrangements for networks such as this. Therefore, the needs of terms procedures, passwords, firewalls and cryptographic equipment would be on the better track. Wireless systems are slightly different, however, as there is no physical connection between the components. Communications can be conducted by mobile terminals which use of low powered UHF radio frequency to communicate with peripheral devices or with a central server[15] and such systems are

---

14. - "NATO and Cyber Defence," North Atlantic Treaty Organization. p. 1. September 16, 2011. http://www.nato.int/cps/en/SID-70CBB31B-8D6C1F24/natolive/topics_78170.htm?

15. - Scot Valdmeir.` Information : Threat and Possibilities' ASEAN- ISIS, issue No 11, Jun 2001,p 55

now frequently within the civil markets, the penalty that should be paid for the added flexibility of using a wireless network is that this creates additional security problems. Another areas of interest is the infrastructure, which includes all of the telecommunications infrastructure within country or geographic area such as telephone switches, satellite communications equipments, fiber optic cablings, microwave relay stations and other relating elements. Since the infrastructure is such a large and complicated asset, it is typically owned and operated by government or collections of independent telecommunication. However, when dealing with security of the infrastructure, the thinking about things such as ensuring that it is free from interference or compromise by foreign power.

Thirdly, components deals with systems security and this primarily relates to the operating systems. We could see how the ongoing on the security of Microsoft new Windows XP operating systems.[16] Within days of its release, substantial flaw was discovered in the security of the product and several patches have since been released to the rectify problems. Regardless of whether the used of other Operating systems (OS) such as Win XP and NT, each OS has its own security systems architecture. The system should be the best defence tools that could be implemented or to be used in the present military establishment. However, it is better to have operating systems which have more than one level of security.

OFFENSIVE CYBER WARFARE

The offensive cyber warfare is consider as the opposite way to counter the cyber threat in which there are an enormous number of tools which can be used to mount an attack on target within cyber space. This technique has been applied in Gulf War between Iraq and Coalition Force in 2003, and as the result of disabling air defence systems, sending missiles off-course, interfering with soft ware or causing catastrophic hardware. This attack has destroyed all electronic and computer systems of the Iraqi that was jammed by the Coalition Forces led by the US.[17] A Chinese journalist has referred to how a `digitized force', might be attacked once a set of communication equipments has been obtained, after which enemy information can be stolen or falsified.[18] This concept also being used outside the military sphere, such as the alteration and stolen of money in bank accounts at Canadian Bank in 1999, where cyber attack applied the technique of password attacks using the combination of computer banking systems incorporated with Seattleite systems.

Other ideas of cyber warfare attacks are more manipulative, interfering with the content of information processes rather than their form. `Semantic Attacks' are another way of cyber attacks with allows an external agent to control as system that appears to

---

16. Ibid, p. 60.

17. James Dunn, `Gulf War: Electronic Perception' Pacific Review. Vol 7,no 4, 1996,p 23.

18. Bernard S. Kim` Digital World: Force and Equipment', International Affairs, Vol 18,(fall),p 45.

insiders to be working normally. Television images might be distorted by the power of cyber war to make opponent political leaders appear ridiculous and misleading in their actions; these actions could be sent through satellite and could be spread throughout the society to another.

CONCLUSION

No protection is perfect. The completely secure system can never be accessed by anyone. Isolation is hard to enforce, therefore systems must use firewalls, encryption and other known defense mechanisms to be protected from terrorism. Exclusively using electronic methods for terrorism is still a few years into the future, but now is the time to find better defense mechanisms.

The more that technology becomes an integral part of our society the more we must ensure that there is enough human supervision and intervention to protect those whom the technology serves. This can be done by raising security readiness to its highest threshold, and also by constantly improving policies, performance, and reviewing security programs. With better protection, users of computer systems will be in a better position to prevent and respond to cyber terrorism.

As computer technology has become increasingly integrated into modern military organisations, military planners have come to see it as both a target and a weapon, exactly like other components and forces. Like other elements of the modern military, cyber forces are most likely to be integrated into an overall battle strategy as part of a combined arms campaign.

BIBLIOGRAPHY

BOOKS

1. Badsey, Stephen., The Conceptual Origins of Information Warfare, Global Transformation Research Group, 1999, London.
2. Campen, Alan D. Dearth, Douglas H. and Goodden, R. Thomas. Cyberwar Security and Confict in the Information age, Armed Forces Communications and Electronics Association USA, Tarun Offset Printers, Delhi.
3. Denning, Dorothy E. Information Warfare and Security, ACM Press Books, 1999, England.
4. Denning, Dorothy E. and Denning, Peter J. Internet Besieged, Countering Cyberspace Scofflaws, ACM Press, 2000, New York.
5. Edited by Malik, J. Mohan. The Future Battlefield, Deakin University Press, 1997, Australia.

6. Edited by Pfaltzgroff, Robert L. and Shultz, Richard H. War in the Information Age: New Challenges for US Security, Brassey's Book, 1997, USA.
7. Erbschloe, Michael. Information Warfare, Osborne/McGraw-Hill, 2001, California.
8. Hutchinson, Bill and Warren, Matt. Information Warfare, Butterworth Heinemann, 2001, Auckland.
9. Keegan, John. History of Warfare, Alfred A. Knopf, 1994, New York.
10. Khor M. Globalization and The South, Malaysia, Jutaprint, 2000, Pinang.
11. Libicki, Martin C. Seven Types of information Warfare, Strategic Studies Institute, US Army War College.
12. Marett, Paul. Information Law Practice, Ashgate Publishing Limited, (Second Edition 2002), England.
13. Rowley, Jennifer and Farrow, John. Organising Knowledge, US, Gower Publishing Ltd, 2000, United States of America.
14. Schwartau, Winn. An Introduction to Information Warfare, Brassey's Book, 1997, United States of America.
15. Shimeall, Timothy. William, Phil and Dunlevy, Casey. Countering Information Warfare, Web edition, NATO Review, 2000.
16. Vakki, Pertti. Savolainen, Reijo. And Dervin, Brenda. Information Seeking in Context, Taylor Graham, 1997, United Kingdom.

JOURNALS AND NEWS PAPERS

1. Armed Forces Journal, International, Space Spy, July 2002,p50.
2. Malaysian Science and Technology Indicators Report 1998, Malaysia.
3. Kol Mohd Yusof bin Hj Sharon, The Integration of Data Network in the Malaysian Armed Forces Through the Use of Corporate Information Superhighway (COINS), 'SOROTAN DARAT – T3029', June 2000 'JILID BIL 35', Ministry Defence Malaysia, p15.

WEB SITE

1. Hayes, Richard E. and Wheatley, Gary. Threats and Challenges http://www.ndu.edu/inss/strforam.html, accessed on 25 March 2003.
2. Lt Col Fast, William R. Knowledge Strategies: Balancing Ends, Ways and Means in The Information Age, http://www.ndu.edu/inss/siws/ch1n html, accessed on 2 March 2003.
3. MAMPU Hompage, http://www.mampu.gov.my, MyMIS Handbook, 2000, accessed on 25 March 2003.

4. McNair, Right Makes Might: Freedom and Power in the Inrormation Age, Chapter one, http://www.ndu.edu/inss/strforam.html. Accessed on 25 March 2003.
5. NISER Homepage, Security Breach Statistic, http://www.niser.org.my. Accessed on 25 March 03.
6. Sohaimi Mohd Salleh (Waseda University), Malaysia's National Information Infrastructure: Issues and Challenges of the Multimedia Super Corridor (MSC), http://www.fas.org/index.shtml, accessed on 25 March 2003.
7. Molander, Roger C. Riddile, Andrew S. and Wilson, Peter A. (1996). Strategic Information warfare: A New Face of War, http://www.ndu/inss/strforum/html.
8. Round, W. Oscar, and Rudolph, Jr, Earle L. (September 1995), Difining Civil Defence in the Information Age, http://www.ndu/inss/strforum/html.

Kapt Sathiyaah a/p Asokumar (3010405) telah ditauliahkan ke memegang jawatan Ketua Platun di 7 Komp KPTD, Ketua Platun di 101 Komp KPTD dan Pegawai Staf 3 Provos di MK Medan TD. Beliau berkelulusan Ijazah Sarjana Muda Sains Komputer dari UTM. Beliau kini berkhidmat sebagai Ketua Platun di 102 Komp KPTD.

PENDAHULUAN

Perang Iran-Iraq bagi masyarakat Arab juga dikenali sebagai Perang Pertahanan Suci. Di Iran ia dikenali sebagai Perang Revolusi Iran manakala di Iraq pula dikenali sebagai Qadisiyyah Saddam. Peperangan antara kedua-dua negara telah bermula pada bulan September 1980 dan berakhir pada bulan Ogos 1988. Umumnya perang ini juga dikenali sebagai Perang Teluk Parsi sehingga timbul konflik Iraq-Kuwait pada awal 90 an dan untuk beberapa ketika ianya dikenali sebagai Perang Teluk Parsi Pertama.

Peperangan ini bermula apabila Iraq menceroboh sempadan Iran pada 22 September 1980 berikutan perebutan sempadan yang berterusan dan juga atas desakan penggulingan rejim Saddam Hussein, di mana Iran telah menyokong rancangan tersebut. Tentera Iraq telah menyerang dan menawan Iran. Namun serangan tersebut telah berjaya ditangkis oleh Iran. [1]PBB telah memohon dan menyeru agar gencatan senjata dilaksanakan namun pertempuran tetap berterusan sehingga 20 Ogos 1988. Kesan peperangan telah mengubah keadaan politik serantau dan dunia. Ia juga turut melibatkan penggunaan senjata kimia oleh tentera Saddam ke atas pasukan Iran dan juga etnik Kurdis Iran. Peperangan ini juga menunjukkan kesan kenaikan harga minyak yang telah mempengaruhi perkembangan ekonomi serantau dan dunia khasnya.

Esei ini akan membincangkan bagaimana peperangan ini timbul dan sebab sebenar ia tercetus dan kesannya pada masa kini. Skop perbincangan ini juga akan merangkumi perhubungan kedua-dua negara terhadap kuasa besar barat seperti Amerika dan Israel merangkumi aspek politik, peranan kuasa besar dalam membekalkan peralatan ketenteraan, teknologi serta ekonomi. Esei ini juga bertujuan untuk menganalisa kesan peperangan Iran-Iraq terhadap ekonomi Timur Tengah serta mengenal pasti peranan Amerika Syarikat sebagai pencetus utama perang ini.

PERHUBUNGAN IRAN - IRAQ DENGAN KUASA BESAR BARAT

Sejarah awal, Iran merupakan sebuah negara yang mempunyai persamaan di dalam kebudayaan dan menggunakan bahasa Parsi. Ketika itu, negara-negara ini diperintah oleh empayar seperti Medes, Achaemenid dan Sassanid iaitu sebelum

1. Rencana bebas. Perang Iran – Iraq m.s 2.

kedatangan Islam[2] . Nama Parsi ini sebenarnya diambil dari perkataan “Fars” menerusi bahasa Greek, negara-negara Eropah juga menamakan Iran sebagai Parsi. Pada lewat kurun ke 19, Iran memasuki sebuah era baru dengan terjadinya Revolusi Perlembagaan sistem beraja berpelembagaan iaitu sebuah pemerintahan moden. Sebuah parlimen yang dinamakan “Majles” ditubuhkan pada 07 Okt 1906.

Namun begitu, penemuan minyak mentah di kawasan yang di kenali “Khuzestan” telah menarik minat pihak British dan Russia untuk meluaskan pengaruh mereka di Iran. Kedua-dua kuasa besar ini bersaing untuk memonopoli hasil minyak Iran dan akhirnya memecah belahkan Iran. Ketika perang dunia pertama, Iran terletak di bawah pengaruh British dan Rusia walaupun polisi kerajaannya adalah neutral. Pada tahun 1919, British cuba menjadikan Iran sebagai negara di bawah naungan mereka, tetapi perancangan tersebut terbantut apabila **Shah Reza**[3] menggulingkan kerajaan Qajar dan menubuhkan “Dinasti Pahlavi”. Beliau memerintah selama 16 tahun dan memulakan proses pemodenan Iran serta menubuhkan kerajaan sekular baru.

HUBUNGAN ISRAEL-IRAN

Iran juga telah mengadakan hubungan yang baik dengan kerajaan Israel yang merupakan sekutu kuat bagi pihak Amerika. Pada 2 Jan 1985 mereka telah membeli senjata-senjata dari Israel yang dianggarkan bernilai 164 bilion dollar US dengan pertukaran minyak dari Iran[4]. Selain itu, dengan peristiwa terjadinya letupan kapal terbang Argentina yang membawa stok senjata dari Tel Avis ke Tehran melalui Qabras juga telah membuktikan kesahihan perjanjian tersebut[5].

Kenyataan secara terbuka pihak akhbar dan kerajaan Yahudi telah menyemarakkan lagi berita[6] tersebut seperti contoh berikut:

a. Sumber maklumat Perancis menegaskan jumlah Yahudi Iran memasuki Palestin melalui Vienna dengan purata 600 orang Yahudi seminggu serta mencecah seramai 9000 orang sejak tahun 1983.

b. Perdana Menteri Israel mempertahankan jualan senjata kepada Iran dan menyatakan Iraq lebih merbahaya daripada Iran terhadap Israel dan Amerika.

c. Yahudi Iran telah mendermakan 70 bilion riyal kepada Iran untuk kepentingan peperangan dengan Iraq.

---

2. Ensiklopedia bebas. Sejarah Iran m.s 1.

3. Shah Reza Pahlavi Raja Iran pada tahun 1935.

4. Patrick Clawson. External Iran m.s 5.

5. Ibid m.s 6.

6. Ibid m.s 8.

d. 14 Feb 1983 pertemuan mesra antara Khomenni dengan pemimpin Yahudi di banggunan Majlis Syura untuk membincangkan hubungan diplomatik serta hala tuju kedua-dua negara[7].

e. Sekumpulan pegawai senjata Israel telah mengadakan kontrak dengan Tehran serta mengikat perjanjian sehingga gaji yang mencecah 10,000 dolar Amerika bagi setiap orang untuk kerjasama di Iran.

Inilah bukti bahawa Iran juga mengadakan hubungan yang baik dan erat dengan Israel di dalam strategi memerangi kerajaan Iraq. Dengan pengabungan dan penggunaan teknologi Israel, Iran berharap dapat memenangi peperangan dari Iraq. Namun dipihak Israel pula mereka merancangkan agar hubungan ini dikekalkan bagi merealisasikan perancangan menguasai Timur Tengah dan terus memecah belahkan kedua-dua negara ini yang pasti akan mengancam kepentingan kuasa besar barat di Timur Tengah.

HUBUNGAN AMERIKA-IRAN

Walaupun permusuhan yang ditunjukkan oleh Iran terhadap Amerika yang disifatkannya sebagai syaitan besar, namun terdapat hubungan yang erat dan mendalam antara Amerika dengan pemimpin-pemimpin Syi`ah sejak tahun 40-an lagi. Terdapat juga beberapa janji lama Amerika kepada pemimpin Iran untuk mendirikan negara Syi`ah. Perjanjian-perjanjian ini dibuat kerana Amerika merasakan apabila tertegaknya sebuah negara Islam untuk Ahli Sunnah di salah sebuah negara Timur Tengah seperti Mesir, Syria atau Iraq, maka pasti pertubuhan-pertubuhan lain akan menyertainya. Ini akan menimbulkan kewujudan bahaya besar terhadap barat dan Israel. Bagi menafikannya, Amerika dan Israel perlu mendirikan negara Syi`ah yang taksub seperti Iran untuk merealisasikan beberapa matlamat strategi mereka.

Antara bentuk-bentuk kerjasama antara Amerika dan Iran ialah seperti kapal terbang dan senjata Amerika yang tiba di Tehran pada 14 September 1985[8]. Amerika juga menghantar dan membekalkan roket-roket Hawk jenis dari bumi ke bumi dalam tempoh yang sama. Khomeini sendiri juga ada mengarahkan supaya diadakan hubungan baik dengan Amerika untuk mengurangkan kedudukan golongan sederhana di Iran. Pada 2 Januari 1985 telah mendedahkan penjualan senjata Israel kepada Iran yang dianggarkan sebanyak 164 bilion dollar US dengan pertukaran minyak Iran. Penjualan senjata Israel kepada Iran di sepanjang tahun (1980-1987) juga dilaporkan daripada Perdana Menteri Israel, Syamir sendiri tentang bantuannya kepada Iran. Israel percaya peperangan yang berterusan melemahkan Iraq, musuh tradisi Israel. Didapati juga bangsa yahudi Iran juga telah mendermakan 70 bilion riyal untuk membiayai kepentingan peperangan dengan Iraq.

---

7. Pemimpin Revoulusi Islam Iran.

8. Dr. Ahmad Al-Afghan. Menyingkap komplot Israel, Amerika dengan Iran. m.s 1.

bangsa yahudi Iran juga telah mendermakan 70 bilion riyal untuk membiayai kepentingan peperangan dengan Iraq.

Kerajaan Iraq pula adalah hasil gabungan kerajaan Mesopotamia (Gabungan Lembah Tigris-Euphrates, Iraq moden dan tanah tinggi di timur iaitu Parsi). Kekayaan di kawasan Khuzestan merupakan jawapan kepada perpecahan di antara Iraq dan Iran. Kerajaan Turki dan panglimanya iaitu Murad IV telah menawan Baghdad dari kerajaan Parsi pada 1638. Perebutan sempadan kawasan di antara Parsi dan Ottoman tidak pernah berubah sehinggalah Brittish berjaya memperolehinya, setelah kejatuhan kerajaan Ottoman di dalam perang dunia pertama.

Saddam Hussein adalah satu watak yang amat anti kepada kerajaan Iran yang mana beliau menganggap bahawa Khuzestan iaitu sebuah wilayah yang kaya dengan minyak adalah di bawah jajahan Iraq serta telah dirampas oleh Iran. Mereka telah menyatakan secara bertulis dan melalui penyiaran radio ke atas pencabulan hak mereka. Pada 1971 Iraq telah memutuskan hubungan diplomatik dengan Iran. Mereka juga telah melancarkan serangan pertama ke atas Iran pada 1974 dan kedua-dua negara ini menghadapi masalah kecelakaan yang teruk.

HUBUNGAN AMERIKA-IRAQ

Mulai 1981, kerajaan Iran dan Iraq telah melancarkan serangan ke atas pelantar minyak dan kapal-kapal perdagangan. Ini termasuklah kepada negara-negara yang berkecuali[9]. Sebagai contoh, setelah kerajaan Iraq melancarkan serangan ke pulau Khark yang merupakan kawasan eksport utama minyak Iran. Iran pula telah menyerang balas pelantar minyak di Kuwait dan Arab Saudi. Serangan ke atas kapal perdagangan di telok Parsi juga telah meningkat.

Pada 1982 setelah Iran berjaya mendominasi peperangan tersebut, pihak Amerika telah membantu kerajaan Iraq dengan membekalkan maklumat, bantuan ekonomi, menguatkan kerajaan dan membekalkan senjata kepada Iraq bagi mengimbangi kekuasaan Iran. Atas desakan dan serangan dari Iran, negara-negara yang berkecuali dan mempunyai keutamaan hasil minyak telah meminta bantuan Amerika untuk menangani dan membalas ke atas tindakan pihak Iran. Amerika telah melancarkan serangan secara besar-besaran keatas kerajaan Iran dan ini telah banyak membantu Iraq sebagai sekutu untuk menangani masalahnya terhadap Iran.

PERANAN KUASA BESAR DI DALAM MEMBEKALKAN PERALATAN KETENTERAAN

Kedua-dua negara teluk yang berperang ini (Iran-Iraq) adalah 2 buah negara yang kaya dengan hasil galian utama dunia iaitu minyak mentah. Mereka berkemampuan untuk memiliki kesemua peralatan yang dikehendaki untuk tujuan peperangan. Hal ini telah membuka mata kuasa besar seperti Amerika untuk mengambil kesempatan bagi

9. Ibid m.s 2

mempromosi semua barang-barang peralatan ketenteraan dan menukarkan produknya yang banyak itu dengan hasil galian yang utama iaitu minyak mentah yang sangat dikehendakinya. Dengan mengagihkan stok peralatan peperangannya yang telah sedia ada serta bersengkongkol dengan sekutunya, ia akan mengembangkan ekonomi kuasa besar seperti Amerika dan mengekalkan setiap peralatannya dilanggani dan diperlukan pada sebilang masa.

Iran pada awal peperangan telah menggunakan peralatan-peralatan dari Syria, Libya, Korea Utara dan China. Namun pada tahun 1985, Amerika melalui sekutunya iaitu Israel telah berjaya memonopoli dan mempengaruhi Iran untuk membeli semua peralatannya melalui Israel. Dianggarkan sebanyak 2,008 (BEM – 71 TOW) iaitu anti tank misil, MLM – 23 Hawk (permukaan bumi ke udara misil), 18 kali F-4 Phantom II kapal pengebom, A – 4 Skyhawk, tank M 60, peluru artileri dan juga alat ganti yang dianggarkan melebihi 2 billion dollar Amerika. Selain itu pesawat pejuang dan helikopter penyerang seperti F – 4, F – 5 dan AH-I Cobra. Semua ini adalah melalui sekutu Amerika secara terus iaitu Israel. Di mana pertukaran peralatan ini adalah secara pemberian hasil minyak kepada mereka[10].

Manakala, pihak tentera Iraq pula kebanyakan peralatan ketenteraan banyak dimonopoli oleh kerajaan Soviet Union dan sekutunya. Sebagai contoh Scud, misil dari Soviet Union. Iraq juga memperkukuhkan tenteranya dengan pesawat pejuang seperti MIG (21, 23 dan 25), Sukhoi SU-22s dan Dassault Mirage F1s dari Perancis[11]. Walau bagaimanapun, Amerika tetap memperolehi tempat dalam membekalkan Iraq dengan teknologi senjata kimia dan biologi dan juga membekalkan kebolehan senjata nuklear kepada Iraq.

Dari segi faktor membekalkan peralatan ketenteraan, Amerika dan Israel adalah kuasa besar utama yang merancang perolehan senjata kepada kedua-dua negara yang bertelagah ini. Iran dimonopoli oleh Israel menakala Amerika walaupun tidak kesemuanya, namun tetap mendapat tempat di dalam membekalkan teknologi senjata nuklear dan senjata kimia yang merupakan sumber utama pengagihan minyak Iraq kepadanya. Kedua-dua negara memainkan peranan supaya penguasaan minyak secara berterusan dan pengukuhan ekonomi di Timur Tengah di teruskan dengan cara yang halus dan teliti malah, mengucar kacirkan hubungan kedua-dua negara.

TEKNOLOGI

Secara keseluruhannya, bagi Iran, teknologi persenjataannya telah dikuasai oleh Israel yang merupakan sekutu Amerika. Ianya bermula dari senjata kecil sehinggalah kepada misil. Namun dipihak Iraq, negara-negara seperti Soviet Union dan China adalah merupakan penyumbang terbesar kepada teknologi mereka.

10. Rencana Amerika support for Iraq – Iran war. m.s 1.

11. Ibid m.s 3

Namun begitu di Iraq, Amerika Syarikat tetap dapat membekalkan persenjataan walaupun pada bilangan yang kecil. Teknologi senjata kimia dan biologi yang ada pada mereka telah dimasukkan ke dalam pengaruh tentera Iraq. Senjata kimia seperti gas sarin dan mustard yang diperolehi dari Amerika telah digunakan untuk memerangi tentera Iran. Amerika juga membekalkan teknologi senjata biologi kepada Iraq dengan firma-firma agensinya mengeksport mikroorganisma dan hasil kajian biologi oleh kerajaan Amerika kepada Iraq[12]. Walau bagaimanapun Iraq tidak menggunakan senjata ini ke atas Iran walaupun ia memiliki kemampuan untuk menggunakannya.

EKONOMI

Ekonomi merupakan faktor utama untuk kerajaan Amerika datang ke Asia Timur Tengah. Amerika telah membuat perkiraan jika ia dapat mempengaruhi dan menguasai negara di Asia Timur Tengah ini, ia akan dapat menentukan sumber ekonomi Amerika dari minyak mentah dan dunia di dalam genggamannya. Ia akan menentukan kepentingan minyak di perolehi dengan mempergunakan Saddam Hussein bagi memerangi Iran serta mengaut keuntungan dari kedua-dua negara ini. Dengan kata lain menguasai ekonomi dan minyak di Timur Tengah adalah tujuan utama Amerika[13] .

Amerika Syarikat juga sanggup mengeluarkan belanja yang tinggi dan mencecah bilion dollar di dalam membantu negara-negara yang berkecuali dan berkepentingan minyak. Ini kerana mereka tahu dengan kejayaan menguasai dan berkerjasama dengan negara-negara ini akan memberi pulangan yang lebih lumayan dan membantu mereka membiayai semula pelaburan yang telah dilaksanakan serta mengembang penguasaan mereka di serata pelusuk dunia.

Di dalam mencetuskan peperangan dan ketegangan ke atas kedua-dua negara tersebut, kerajaan Amerika juga dapat mengaut keuntungan pertukaran minyak dengan teknologi senjata dan kepakaran yang sedia ada padanya. Di sini sebagai contoh Amerika dan sekutunya Israel telah membantu kedua-dua negara untuk memiliki persenjataan, aset kereta kebal dan kapal terbang untuk memerangi sesama mereka namun pertukaran ini adalah melibatkan hasil galian yang utama iaitu minyak mentah.

KESAN PEPERANGAN

Pertubuhan Bangsa-Bangsa Bersatu menyeru untuk gencatan senjata, pertempuran tetap berterusan sehingga 20 Ogos 1988. Manakala, tawanan perang terakhir ditukar pada tahun 2003. Kesan peperangan juga mengubah politik serantau dan dunia. Ia juga turut menyaksikan penggunaan senjata kimia oleh tentera Saddam ke atas pasukan Iran dan juga etnik Kurdis di Iran. Dianggarkan seramai 500,000 tentera dan awam telah

---

12. Ibid m.s 7 dan 8.

13. Lt Kol Toh Choon Siang. Kertas kerja MPAT. Dimension of Strategy Adopted by The Coalition Forces During The 1st Gulf War And Their Significance m.s 8.

terkorban di pihak Iran manakala 375,000 di pihak Iraq. Harga minyak mentah melonjak dari 40 dollar setong sebelum peperangan dan telah meningkat sehingga 70 dollar setong selepas peperangan. Kedua-dua negara tersebut rosak dari segi muka bumi, eko-sistem, peradaban dan kemanusiaan dengan pembunuhan yang berterusan. Ianya menambah dan menjadikan dunia lebih parah dengan kerosakan yang dilakukan oleh kuasa-kuasa lain seperti Russia, Britain dan Perancis, bukan setakat peperangan tetapi juga dengan ujian-ujian nuklear, terutama di bawah tanah, penerokaan, pencemaran dan penjelajahan di angkasa lepas dan pencemaran serta kerosakan dimuka bumi. Hakikat sebenarnya, keganasan berlaku ialah hasil dari tindakan kuasa-kuasa besar yang menjajah, mengeksploitasi dan menguasai negara secara kekerasan. Contohnya penguasaan Amerika terhadap Iraq dan Israel terhadap Iran jelas tidak berperikemanusiaan dan memaksa mengikut kemahuannya ke atas orang lain.

PENGAJARAN

Beberapa pengajaran yang boleh didapati dari peperangan ini adalah seperti berikut:

a. Penggunaan senjata kimia dan biologi telah mencatatkan tragedi kepada kematian rakyat diantara kedua-dua negara yang berperang. Dianggarkan hampir 875,000 iaitu sebanyak 500,000 di pihak Iran manakala 375,000 bagi pihak Iraq manusia telah terkorban di dalam kancah tersebut dengan penggunaan gas sarin dan mustard kepada tentera serta orang awam dan korban ini merupakan korban perang kedua yang terbanyak selepas Hiroshima dan Nagasaki di Jepun di dalam perang dunia kedua.

b. Untuk beberapa lama kerajaan Iraq dan Iran berjaya mentadbir negara mereka sendiri dan hidup dalam kebebasan. Namun dengan campur tangan dari Israel dan Amerika telah memecah belahkan negara mereka. Kehadiran Amerika untuk membantu Iraq adalah sebenarnya untuk memperolehi keuntungan mereka di dalam penjualan senjata dan teknologi hingga menyebabkan kehilangan ramai nyawa diantara kedua pihak. Iraq yang dulunya sekutu Amerika telah di perangi oleh mereka kembali sehingga Saddam Hussein yang menjadi kepercayaan Amerika telah di guling serta di bunuh atas konpirasi yang telah dicipta oleh pihak barat sendiri. Rakyat Iraq pula terus menderita serta pencerobohan ke atas negara mereka berterusan sehingga kini.

c. Kekayaan minyak di kedua negara telah menyebabkan terdapanya campur-tangan kuasa asing untuk menguasai hasil galian dan membawa keuntungan kepada mereka. Khuzestan merupakan wilayah Iran manakala Kirkuk di pihak Iraq. Namun di atas desakan dan hasutan Amerika yang memutarbelitkan fakta dan ideologi menyebabkan tercetusnya perbalahan diantara keduanya hingga tercetus kesusahan dan kesengsaraan kepada rakyat.

d. Dasar luar Amerika yang menegaskan akan memerangi penganas telah berjaya menjadikan negara Iran sebagai satu ancaman kepada kesejahteraan sejagat dan boleh menggugat serta patut diperangi. Ini menyebabkan Iraq mempercayai dengan memerangi Iran ia berpendapat akan menguasai Timur Tengah namun prinsip itu telah memudahkan Amerika dan sekutunya menguasai Asia Timur yang kaya dengan minyak kerana setelah berjaya mempengaruhi kedua-dua negara kuasa barat telah memanipulasikan fakta untuk menghancurkan sekutu yang telah membantunya itu sehingga menyebabkan berlaku pencerobohan terhadap Iraq yang dikatakan mempunyai kuasa nuklear yang boleh mengancam dunia.

e. Kekurangan sumber dan kemampuan senjata serta ideologi telah menyebabkan kuasa besar seperti Amerika dan Israel telah berjaya memecahbelahkan Iraq dan Iran dan menyekat mereka dari bersatu. Pihak barat juga dapat menyedut hasil utama kedua negara iaitu minyak mentah dan mengembangkan pengaruh mereka di Asia timur amnya serta dunia khasnya.

PENUTUP

Amerika syarikat telah berjaya memecah belahkan dua buah negara Arab yang kuat dan kaya dengan sumber ekonomi dengan dasar propagandanya bagi mengaut keuntungan dengan hasil jualan senjata serta teknologinya kepada kedua-dua negara tersebut. Penguasaan negara Iran melalui sekutunya iaitu Israel manakala Iraq pula oleh Amerika sendiri. Faktor penguasaan ekonomi adalah menyebab utama untuk Amerika datang menguasai Iran dan Iraq kerana mereka percaya dengan penguasaan hasil minyak ia akan dapat mengimbangi kuasa monopoli di Asia Timur serta membantunya menguasai dunia melalui penambahan hasil ekonomi yang diperolehinya dari minyak kedua-dua negara.

Kegagalan Iraq dan Iran bersatu telah menyebabkan kuasa besar barat mengambil kesempatan untuk melagakan mereka kerana barat berpendapat jika dua buah negara yang kaya dengan minyak mentah ini dibiarkan bersatu ia akan menjadi sebuah kuasa baru di Asia Timur serta akan menggugat mereka. Iraq dan Iran kini telah bertukar menjadi musuh Amerika serta kini diperangi pula oleh sekutunya yang dulu membantu dan kini menekan mereka dengan alasan mempunyai teknologi nuklear yang mengancam dunia. Manakala negara Iraq pula terlibat didalam konflik peperangan sehinggalah sekarang dan rakyat menjadi pelarian di negara sendiri manakala bekas presiden iaitu Saddam Hussein di bunuh tanpa pembelaan yang sewajarnya. Rakyat Iraq dan Iran terpaksa menerima kesan yang amat perit dan teruk hasil perbalahan dan mempunyai pemerintah yang lemah serta mudah dipengaruhi. Keadaan ekonomi yang teruk serta kemudahan yang terhad menyebabkan mereka tiada pilihan dengan menerima bantuan dan pendapat dari kuasa asing. Sesungguhnya peperangan ini telah menyatakan Amerika dan sekutunya telah memenangi dan menguasai ekonomi di Timur Tengah serta dunia, namun telah kalah di dalam mengembalikan keamanan kepada kedua-dua negara yang bergolak ini.

BIBLIOGRAFI:

1. Ensiklopedia Bebas. 11 Jan 2008. Saddam Hussein,http://ms.wikipedia.org/wiki/saddamHussein.
2. Dr. Shafie Abu Bakar. 31 Jan 2005. Mendepani Kuasa Unipolar.
3. Ensiklopedia Bebas. 31Jan 2005. Perang Iran-Iraq, http://ms.wikipedia.org/wiki/Perang Iran Iraq.
4. Dr. Ahmad Al-Ghani. 18 Mac 2007. Menyingkap komplot Israel/Amerika Dengan Iran.
5. Matthew White. 3 Mac 2003. First Gulf War.
6. Ensiklopedia Bebas. 10 Dis 2007. Sejarah Iran, http://ms.wikipedia.org/wiki/Sejarah Iran.
7. Toh Choon Siang. Lt Kol. MPAT 23/2003. Dimension Of Strategy Adopted By Coalition Forces During The 1st Gulf War And Their Significanse.

PW II Anuar bin Abdullah telah mula berkhidmat ke dalam Kor Polis Tentera Darat pada 1 Jul 1997. Berkelulusan sehingga Tingkatan 5 (SPM). Unit pertama beliau ialah di 2 Komp KPTD, Kem Kemunting Taiping, Perak. Bertukar ke PULAPOT pada tahun 2007 sebagai KMSK AM. Beliau kini berkhidmat sebagai KMSR di Cawangan Kuartermaster pasukan 4 Rejimen KPTD, Kem Sungai Buluh sehingga sekarang

SEJAUH MANAKAH KEBERKESANAN PENGURUSAN ASET DALAM TENTERA DARAT

oleh Kapt Tengku Norazlinawaty bt Tuan Hamzah

Angkatan Tentera Malaysia (ATM) merupakan suatu organisasi yang besar dimana tanggungjawab yang diberikan tidak hanya mempertahankan negara pada masa aman, darurat mahupun perang semata-mata. Salah satu tanggungjawab sampingan yang perlu dilaksanakan oleh ATM pada masa aman adalah menentukan Pengurusan Aset Kerajaan dilaksanakan secara berintegriti bagi mengelakkan kerugian kepada kerajaan. Aset bermaksud harta benda kepunyaan, milikan atau di bawah kawalan kerajaan yang dibeli atau yang disewa beli dengan wang kerajaan, yang diterima melalui sumbangan, hadiah atau diperolehi melalui proses perundangan. [1]Aset juga merupakan harta yang mempunyai nilai dan boleh dijual atau dipindah milik. Pengurusan Aset Kerajaan adalah merupakan proses yang mana melibatkan penerimaan, pendaftaran, penggunaan, penyimpanan, pemeriksaan, penyelenggaraan, pelupusan, laporan kehilangan serta hapus kira. Proses-proses tersebut dilaksanakan terhadap harta berbentuk fizikal yang mempunyai nilai dan diperolehi sama ada untuk digunakan terus atau bagi masa akan datang dalam pengeluaran barang siap atau perkhidmatan.

Aset-aset yang tersimpan di dalam stor merupakan modal terikat iaitu wang kerajaan yang tersimpan dalam bentuk barangan bagi tujuan memberi perkhidmatan serta kepuasan kepada pelanggan pada kos yang minimum. Kebanyakan punca kerugian yang dialami oleh kerajaan adalah disebabkan daripada pengurusan aset yang lemah, tidak teratur dan tidak cekap. Pengurusan Aset Kerajaan wajar diberi keutamaan oleh Kementerian atau Jabatan kerana ia merupakan aspek penting dalam pengurusan kewangan. Sejajar dengan itu, merujuk kepada Panglima Angkatan Tentera Ke-17, Jeneral Tan Sri Dato' Sri Azizan bin Ariffin TUDM juga telah menekankan kepentingan Pengurusan Aset Kerajaan didalam Perintah Ulung beliau yang berbunyi seperti berikut:

" Dalam memastikan interoperability antara sistem-sistem yang terdapat dalam perkhidmatan-perkhidmatan, salah satu aspek yang wajib diberi tumpuan adalah pada aspek keempat iaitu ***Memartabatkan Pengurusan Aset Dan Budaya Senggaraan****. Sistem pengurusan aset ATM perlu diperkemaskan untuk menjadi lebih sistematik supaya ianya benar-benar menekankan kebertanggungjawaban (accountability). Sistem 'check and balance' antara 'stakeholders' perlu diberi nafas baru dalam menentukan setiap proses perolehan, penginventorian aset, senggaraan dan pembaikan peralatan menepati dan mengikut prosuder yang telah ditetapkan. Ini bermakna pengurusan aset yang kemas akan mengelakkan dari berlakunya ketirisan*

---

1. Surat Arahan Perbendaharaan Bertarikh 24 Sep 2010.

bajet, dan secara langsung akan menjurus kepada kadar kebaikan aset yang tinggi. Budaya kecemerlangan yang mengamalkan prinsip 'Continous Process Improvement' untuk menghasilkan impak secara nilai tambah perlu diterapkan oleh semua peringkat pengurusan dalam ATM [2].

Aset kerajaan dibahagikan kepada 2 kategori iaitu Aset Tak Alih dan juga Aset Alih. Aset Tak Alih merupakan aset yang tidak boleh dialih iaitu bangunan, tanah dan sebagainya. Aset tanah adalah dibawah bidang kuasa Ketua Pengarah Tanah dan Galian manakala bangunan dibawah bidang kuasa Jabatan Kerja Raya (JKR).[3] Pengurusan Aset Kerajaan di dalam Tentera Darat kebiasaannya melibatkan Aset Alih yang mana pengawalan di bawah bidang kuasa Bahagian Kawalan dan Pemantauan Perbendaharaan. Aset Alih terbahagi kepada harta modal, inventori, bekalan pejabat dan juga stok dalam stor. Aset Alih Kerajaan bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan. [4]Harta modal merupakan barang tak luak yang bernilai RM 1,000.00 atau lebih setiap satu pada masa perolehan yang memerlukan penyelenggaraan secara berjadual tanpa mengira harga perolehan asal. Penyelenggaraan secara berjadual merujuk kepada aset yang memerlukan penyelenggaraan seperti yang telah disyaratkan di dalam manualnya.[5] Contoh kategori harta modal adalah seperti jentera berat, kenderaan, peralatan pejabat, sukan, perubatan, kelengkapan ICT dan sebagainya. Inventori pula merupakan barang tak luak yang kos perolehan asalnya tidak melebihi RM 1,000.00 dan tidak memerlukan penyelenggaraan berjadual.[6] Walau bagaimanapun aset-aset alih seperti perabot, hamparan, hiasan, langsir dan pinggan mangkuk adalah termasuk di dalam kategori inventori tanpa mengira nilai perolehan asal. Bekalan pejabat merupakan barang tak luak yang terlalu rendah nilainya serta tidak ekonomi untuk dikesan penempatan satu persatu. Contohnya stapler, gunting, pisau, pen, pemadam, alat pengasah serta segala peralatan alatulis yang digunakan. Dalam keadaan semasa, peraturan mengenai Pengurusan Aset Alih Kerajaan terkandung dalam beberapa dokumen yang berasingan antaranya Arahan Perbendaharaan (AP), Panduan Perbendaharaan-Tatacara Pengurusan Stor (PP-TPS), Pekeliling Perbendaharaan (PP) dan Surat Pekeliling Perbendaharaan (SPP). Oleh kerana terdapat berbagai-bagai dokumen, ianya telah banyak menimbulkan keraguan di kalangan pegawai awam terutamanya mereka yang terlibat dan bertanggungjawab secara langsung terhadap pengurusan aset tersebut. Di samping itu, isu berkaitan kelemahan di dalam Pengurusan Aset Alih Kerajaan sering dibangkitkan dalam Laporan Ketua Audit Negara. Bagi menangani masalah-masalah

---

2. Perintah Ulung Panglima Angkatan Tentera Ke-17.
3. Surat Arahan Perbendaharaan bertarikh 24 Sep 2010.
4. Surat Arahan Perbendaharaan bertarikh 24 Sep 2010.
5. Surat Arahan Perbendaharaan bertarikh 24 Sep 2010.
6. Surat Arahan Perbendaharaan bertarikh 24 Sep 2010.

tersebut dan mengambil kira perkembangan semasa maka semua peraturan berkaitan Pengurusan Aset Alih Kerajaan telah dikaji semula, dikemaskini, diseragam dan digabungkan dalam satu tatacara Pengurusan Aset Alih Kerajaan yang menyeluruh seperti yang terdapat di dalam PP Bil.5 Tahun 2007 yang ditandatangani oleh Ketua Setiausaha Perbendaharaan pada tarikh 2 Mac 2007.

Pada permulaannya, pengurusan aset meliputi perolehan, pendaftaran, penyelenggaraan, pelupusan dan kehilangan. Perolehan adalah satu kaedah yang digunakan dalam mendapatkan atau membeli peralatan, perkhidmatan dan barang kerja yang dikehendaki. Tatacara Perolehan telah ditetapkan dalam Arahan Perbendaharaan (AP 166 hingga 300) yang dikeluarkan oleh kerajaan. Terdapat 3 jenis tatacara perolehan iaitu Perolehan Kerja, Perolehan Bekalan dan Perolehan Perkhidmatan. Perolehan Kerja meliputi tiga jenis bidang untuk diuruskan seperti pembinaan bangunan, pendawaian elektrik, landskap, hawa dingin dan seumpamanya. Perolehan Bekalan pula meliputi perolehan segala jenis alat seperti alatulis, kelengkapan pejabat, mesin, bahan bacaan dan sebagainya. Manakala Perolehan Perkhidmatan meliputi perkhidmatan seperti pengendalian penyelenggaraan, pembaikan dan pembersihan. Perolehan juga mempunyai pengurusan untuk diperolehi seperti cara pembelian runcit, kerja-kerja baik pulih (Requisition) secara sebutharga dan secara tender.

Pendaftaran di dalam pengurusan aset berfungsi sebagai kawalan dan perlu direkod serta didaftarkan pembelian. Objektif pendaftaran adalah untuk membuktikan hak milik pembeli, asas maklumat, tujuan pengesanan dan asas akauntabiliti. [7]Asas-asas bagi merekod Harta Modal, Inventori dan Bekalan Pejabat. Semua harta modal, Inventori dan Bekalan Pejabat boleh dirujuk pada Pekeliling Perbendaharaan (PP) Bil. 2 Tahun 1991 - Penggunaan borang-borang baru bagi pengurusan Harta Modal, Inventori dan Bekalan Pejabat. Pendaftaran perlulah menggunakan borang-borang seperti berikut :

b. Daftar Inventori (KEW 313).

c. Daftar Stok Bekalan Pejabat (KEW 314).

d. Daftar Pergerakan Harta Modal dan Inventori (KEW 315).

Daftar Harta Modal (KEW 312, 312 A). Butir-butir maklumat dalam Daftar Harta Modal ini dibahagikan kepada dua yang merangkumi pengisian berkaitan Kategori dan Jenis harta modal tersebut. Kategori disini contohnya seperti kenderaan, loji, mesin, peralatan dan kelengkapan pejabat. Bagi Jenis pula, sebagai contoh didalam kategori mesin, peralatan dan kelengkapan pejabat adalah seperti kamera, komputer, mesin penyalin, mesin taip dan sebagainya. Selain itu terdapat tiga belas (13) pengisian data berkaitan yang perlu diisikan ke dalam daftar ini merangkumi daripada jenama dan model harta modal tersebut sehinggalah ke ruangan pelupusan.

---

7. Surat Pekeliling Perbendaharaan Bil. 12 Tahun 1995.

Daftar Inventori (KEW 313). Daftar Inventori diperkenalkan adalah untuk merekodkan perolehan dan penempatan inventori. Daftar inventori adalah dalam bentuk kad. Kad-kad hendaklah disusun mengikut jenis inventori dan abjad. Butir-butir yang perlu direkodkan di dalam daftar ini juga merangkumi Kategori dan Jenis inventori. Kategori inventori adalah seperti peralatan/ kelengkapan pejabat dan perabut/permaidani/ langsir. Jenis inventori bagi kategori peralatan/kelengkapan pejabat adalah seperti alat pengira, kipas angin dan sebagainya. Manakala Jenis Inventori bagi perabut/ permaidani/langsir adalah seperti kerusi, meja, langsir dan sebagainya. Sebelas (11) pengisian lain yang terlibat didalam daftar ini adalah daripada ruangan bilangan sehingga tandatangan.

Daftar Stok Bekalan Pejabat (KEW 314). Daftar Stok Bekalan Pejabat diperkenalkan untuk merekodkan segala berkaitan dengan bekalan pejabat. Daftar ini adalah didalam bentuk buku. Maklumat yang perlu dicatatkan di dalam Daftar Stok Bekalan Pejabat adalah jenis, yang mana merangkumi dua iaitu jenis bekalan pejabat barang luak seperti ball pen, gam dan sebagainya. Manakala jenis kedua ialah barang tak luak seperti gunting, stapler dan sebagainya. Pengisian data berkaitan yang seterusnya adalah unit pengukuran, bilangan, nombor pesanan, diterima/dikeluarkan kepada, tarikh, kuantiti terimaan, kuantiti keluaran, baki dan yang terakhir penerimaan.

Daftar Pergerakan Harta Modal Dan Inventori (KEW 315). Daftar Pergerakan Harta Modal Dan Inventori bertujuan untuk merekodkan pergerakan sebarang harta modal atau inventori. Pergerakan yang dimaksudkan adalah pindahan melalui pinjaman atau penempatan sementara. Daftar Pergerakan Harta Modal Dan Inventori adalah dalam bentuk buku. Butir-butir yang perlu direkodkan ke dalam daftar ini adalah meliputi jenis harta modal/inventori, jenama dan model, nombor siri pembuat, nombor siri pendaftaran, bilangan, nama peminjam, tarikh dikeluarkan, tarikh jangka dipulangkan, pegawai pengeluar dan diakhiri dengan catatan.

Dengan berkuatkuasanya Pekeliling Perbendaharaan Bil 5 Tahun 2007, Tatacara Pengurusan Aset Alih Kerajaan (TPA), setiap Kementerian/Jabatan telah diarahkan untuk memindahkan semua maklumat berkaitan Harta Modal dan Inventori di bawah kawalannya bagi tahun 2006 daripada borang lama KEW 312 dan KEW 313 kepada borang baru KEW. PA-2, KEW. PA-3, KEW. PA-4 dan KEW. PA-5 dengan secepat mungkin tidak melebihi tempoh enam (6) bulan mulai dari tarikh pekeliling tersebut dikeluarkan. Semua aset yang dimiliki oleh setiap Kementerian/Jabatan/PTJ tersebut sebelum tahun 2006, disenaraikan didalam Senarai Daftar Harta Modal (KEW. PA-4) dan Senarai Daftar Inventori (KEW. PA-5) yang baru. Manakala maklumat dalam Daftar Stok Bekalan Pejabat Kew 314 dipindahkan ke Kad Kawalan Stok (KEW 300 J3) dan Kad Petak (KEW 300 J4) mengikut Panduan Perbendaharaan-Tatacara Pengurusan Stor.[8]

---

8. Surat Pekeliling Perbendaharaan Bil. 5 Tahun 2007.

Seterusnya peraturan berkaitan Pengurusan Aset yang terkandung di dalam Arahan Perbendaharaan (AP), Panduan Perbendaharaan-Tatacara Pengurusan Stor (PP-TPS), Pekeliling Perbendaharaan (PP) dan Surat Pekeliling Perbendaharaan (SPP) seperti yang berikut adalah dibatalkan:

a. AP Bab II-Kehilangan dan Hapus Kira, hanya peraturan berkaitan barang-barang awam sahaja.

b. PP Bil 3 Tahun 1990, hanya peraturan berkaitan barang-barang awam sahaja.

c. PP Bil 2 Tahun 1991.

d. SPP Bil 7 Tahun 1995.

e. SPP Bil 2 Tahun 1997.

f. SPP Bil 3 Tahun 2002.

g. PP Bil 8 Tahun 2004 hanya para 8-Pengurusan Stor dan Aset sahaja.

h. Panduan Perbendaharaan-Tatacara Pengurusan Stor hanya Bab XIV dan XV sahaja.

Beberapa kelebihan yang dapat dilihat dan ditafsirkan berdasarkan kepada pelaksanaan penggunaan borang-borang baru di pasukan-pasukan TD dengan panduan yang telah dikuatkuasakan melalui PP Bil. 5 Tahun 2007, Tatacara Pengurusan Aset Alih Kerajaan (TPA) ini adalah :

a. Maklumat Semua Aset Pasukan Disimpan Dengan Cara Yang Lebih Teratur Dan Bersistematik. Dengan berkuatkuasanya TPA ini segala dokumentasi atau rekod-rekod berkaitan aset-aset alih di pasukan akan disimpan dengan lebih teratur yang mana seterusnya akan memudahkan rujukan dibuat apabila ada keperluan seperti keperluan maklumat yang mendesak berkaitan nilai keseluruhan pegangan aset di pasukan mahupun nilai satu persatu setiap aset di pasukan. Berlanjutan daripada itu juga, pihak atasan mempunyai peluang yang lebih mudah untuk mengetahui jumlah aset ataupun nilainya yang dipegang oleh pasukan disebabkan susunan dokumentasi yang teratur. Selain itu, pemantauan yang berterusan daripada pihak atasan juga lebih berkesan.

b. Nilai Aset Yang Mudah Ditentukan Dan Dikira Jumlahnya. Didalam proses pendaftaran aset, iaitu bab B didalam PP Bil. 5 Tahun 2007, dengan jelas menunjukkan adanya pengisian yang wajib di ruangan “Harga Perolehan Asal” dimuka depan Daftar Harta Modal KEW. PA-2 mahupun Daftar Inventori KEW. PA-3. Ini menunjukkan pada peringkat awal penerimaan aset lagi, harga bagi sesuatu aset itu telah dapat ditentukan dengan sahihnya. Ini seterusnya memudahkan bagi pengiraan susut nilai aset tersebut kepada sesiapa sahaja yang bertanggungjawab didalam menggunakan, menyimpan atau menyelenggarakan aset tersebut.

c. Kawalan Kewangan Yang Lebih Berkesan. Adalah menjadi hasrat Kerajaan Malaysia agar setiap kementerian dibawah pentadbirannya agar mampu memiliki cara yang lebih teratur, efektif dan menepati kehendak mengikut ekonomi semasa, didalam mengurus setiap perolehan aset kerajaan. Ini seterusnya membolehkan pengaliran keluar kewangan yang diperuntukkan di setiap kementerian berpatutan tanpa berlebihan perbelanjaan dan mencapai objektif perancangan kerajaan mahupun organisasi tersebut sendiri. Di dalam Kementerian Pertahanan, perkara ini adalah menjadi perkara utama agar di setiap Pusat Tanggungjawab dan Pusat Kos berupaya mengumpul maklumat berhubung aset- aset kerajaan yang hendak dibeli dan yang telah dibeli agar kebolehgunaannya ditahap terbaik dengan mengikut garis panduan yang telah dikeluarkan oleh TPA ini.

d. Pencarian Yang Mudah Melalui Pengkalan Data Secara *Hard Copy* Dan *Soft Copy*. Setiap pengaplikasian bagi kemasukan butir- butir sama ada berkaitan harta modal mahupun harta inventori akan dimasukkan kedalam borang yang telah dikeluarkan secara format tersendiri berserta dengan PP Bil. 5 Tahun 2007, TPA ini. Dengan berdasarkan kepada perkembangan teknologi semasa yang berkembang pesat telah membolehkan borang-borang tersebut mampu dimuat turun melalui talian internet seterusnya memudahkan di dalam proses pengeditan dan kemasukan data kedalam borang yang terlibat. Sekiranya data yang diisi disiapkan dengan lengkap, daftar bagi setiap kemasukan akan memudahkan pencarian maklumat berkaitan aset tersebut serta lebih menjimatkan masa mahupun tenaga individu.

e. Garis Panduan Merangkumi Tatacara Pengurusan Stor. Sistem pengurusan stor sedia ada telah dinaik taraf dengan disatukan dibawah sistem Pengurusan Aset Alih Kerajaan dan dikawal melalui borang-barang Kewangan Pengurusan Aset (KEW. PA) yang melibatkan keseluruhan aset termasuk aset Hidup mahupun Aset Tumbuhan. Dan setiap aset dilabelkan selari dengan daftar rekod aset. Sekiranya aset tersebut mengalami kehilangan mahupun kerosakan atau tidak boleh digunakan serta tidak menguntungkan penggunaannya maka memudahkan dibuat hapuskira ataupun dilupuskan melalui jawatankuasa pelupusan aset.

f. Pencarian Maklumat Melalui Rujuk Silang. Dengan adanya pengisian data-data yang tepat dan pendaftaran kemasukan melalui pelbagai cara di dalam Tatacara Pengurusan Aset Alih Kerajaan (TPA) ini dan digabungkan dengan data sedia ada di dalam Borang Angkatan tentera (BAT) sedikit sebanyak dapat membantu pencarian maklumat dengan tepat melalui rujuk silang bagi mengelakkan segala penyelewengan dan kehilangan aset kerajaan. Di dalam pengurusan di bahagian Kementerian Pertahanan amnya, perkhidmatan di dalam Tentera Darat telah lama mengamalkan pengisian data rekod yang terbaik dan lengkap dari segi konsep pengurusan penerimaan, simpanan, senggaraan, pengstoran, pelabelan, pengeluaran dan dokumentasi bagi segala aset alih yang dipegang di dalam Borang Angkatan Tentera (BAT) semenjak Angkatan Tentera ditubuhkan.

g. Pihak Atasan Dapat Mengenalpasti Dan Mengetahui Jumlah Nilai Aset Yang Dipegang Pasukan Secara Berkala Dan Lebih Cepat. Dalam usaha memastikan perlaksaan TPA yang dikuatkuasakan di setiap peringkat jabatan kerajaan dipraktikkan dengan lebih berkesan, Jawatankuasa Pengurusan Aset Alih Kerajaan perlu diwujudkan. Dengan adanya jawatankuasa ini setiap ketua jabatan akan mampu memperolehi maklumat yang terkini dan dikemaskini berkaitan jumlah pegangan atau nilai aset yang dipegang oleh jabatan masing-masing.

Seterusnya kelemahan yang mampu dikenalpasti berlanjutan daripada pelaksanaan garis panduan di dalam TPA ini adalah :

a. Penilaian Kategori Aset Yang Bercampur Dan Kesesuaian Penggunaan Di Dalam TD. Keserasian penggunaan borang-borang menjadi lebih rumit apabila Tentera Darat di bawah Kor yang dipertanggungjawabkan iaitu yang melibatkan logistik terpaksa akan mengkaji kesesuaian terhadap jenis-jenis stor yang terdiri daripada enam jenis stor yang digunakan selama ini sedangkan didalam sistem baru pengurusan aset alih kerajaan ini hanya mengkategorikan aset alih yang terdiri daripada harta modal dan harta inventori. Tatacara merekod di dalam lejar adalah berbeza-beza.

b. Penyeragaman Borang-Borang Yang Gunasama. Hasil daripada penelitian terhadap penyeragaman ini ianya akan merumitkan apabila ianya masih di dalam gunasama yang mana akan merugikan kertas dan borang sedia ada yang telah dicetak khas oleh Tentera Darat sendiri. Tentera Darat akan mengalami kerugian masa penugasan bagi merekod ke atas dua jenis data yang sama tetapi berlainan borang.

c. Kekeliruan Di dalam Menentukan Kategori Aset. Di dalam pelaksanaan TPA ini di pasukan terdapat kekeliruan bagi menentukan kategori aset kerana kategori yang dinyatakan oleh Perbendaharaan kurang sesuai untuk diaplikasikan di dalam organisasi tentera. Ini disebabkan pegangan dan nilai aset di dalam TD khasnya adalah pelbagai dan mengikut kategori stor di pasukan masing-masing. Selain itu, pegangan aset di antara organisasi dalam TD juga sentiasa berlainan. Berpandukan kepada TPA, harta modal adalah aset alih yang harga perolehan asalnya RM 1,000.00 dan ke atas setiap satu dan aset alih yang memerlukan penyelenggaraan berjadual tanpa mengira harga asalnya atau dengan lebih mudah merujuk kepada aset yang memiliki manual/panduan penyelenggaraan kepada pengguna. Walaupun segala definasi diatas adalah agak jelas diterangkan, tetap ada kekeliruan bagi anggota yang merekodkan data bagi aset yang berkaitan di pasukan kerana masih terdapat pasukan yang menetapkan perabot, hamparan, hiasan dan pinggan mangkuk ke dalam senarai harta modal hanya kerana dengan mengambil kira nilai perolehan asal aset-aset tersebut yang agak tinggi.

d. Permasalahan Anggota Di Pasukan Bagi Merekod Berkaitan Harga Aset Terutama Aset Yang Diperolehi Beberapa Tahun Yang Lepas Sebelum Penguat-kuasaan TPA Ini. Memandangkan aspek utama yang ditumpukan adalah berdasarkan harga maka timbul masalah dipasukan dalam merekodkan perolehan aset yang dilaksanakan beberapa tahun sebelum tahun 2006. Perolehan di dalam TD adalah terdiri daripada beberapa sumber seperti melalui depoh utama dan pembelian luar skala. Apabila aset yang diterima daripada depoh utama, pasukan-pasukan tidak akan dapat mengenalpasti harga perolehan asal setiap unit aset tersebut kerana borang BAT L 8 yang digunakan tidak dinyatakan di dalamnya berkaitan harga aset. Ini merupakan masalah utama kepada anggota stor yang merekod penerimaan bagi mengkategorikan aset tersebut kepada harta modal ataupun harta inventori. Maklumat tersebut hanya terdapat di depoh pusat yang melaksanakan perolehan aset berkenaan dan sekiranya ia disemak di sana akan mengambil masa yang agak lama kerana corak rekod masa dahulu yang dilaksanakan secara manual.

e. Kekurangan Latihan Dan Pendedahan Berkaitan Perlaksanaan Penggunaan Borang-Borang Baru Berpandukan Kepada TPA Ini Sebelum Ianya Dikuatkuasakan. TPA ini telah berkuatkuasa sebelum adanya pendedahan serta latihan yang lengkap diberikan kepada anggota mahupun pasukan dan ini menimbulkan banyak kekeliruan yang tidak dijangkakan. Adalah lebih berkesan, sekiranya latihan secara menyeluruh dilaksanakan di peringkat tenaga-tenaga pengajar di pusat-pusat latihan bagi membolehkan adanya segelintir pakar rujuk untuk permasalahan yang dihadapi di pasukan. Semasa didalam proses perancangan perlaksanaan TPA ini lagi, sepatutnya wakil daripada setiap kementerian perlu ada bagi menyatakan corak pelaksanaan pengurusan aset di pasukan yang sedang dilaksanakan dan permasalahan yang mungkin akan dihadapi di pasukan sebenar apabila ia dikuatkuasakan. Ini bagi mengelakkan pertindihan prosedur yang sedia ada dan mengelakkan anggota melakukan dua kali kerja yang sama yang menyumbang kearah objektif yang satu. Selain itu, dengan kekangan masalah keanggotaan yang terhad akan lebih menyukarkan pelaksanaan TPA ini di pasukan melainkan ianya diberikan pendedahan secara menyeluruh dengan lebih awal.

Secara keseluruhannya, pelaksanaan TPA ini mampu memberikan kesan positif dalam aspek pengurusan aset alih kerajaan di pasukan-pasukan TD mahupun di setiap kementerian yang terlibat. Ianya bertepatan dengan objektif kerajaan untuk memantapkan dan memperkemas tatacara pengurusan aset alih yang sedia ada. Walaupun pada peringkat awal pelaksanaannya menimbulkan banyak kekeliruan dan pencanggahan tetapi sewajarnya kita sebagai rakyat tanpa mengira kedudukan dan jenis organisasi yang sentiasa menjadi tulang belakang kepada kerajaan, berfikir secara positif demi kearah pembangunan pengurusan aset alih ini dengan bersama-sama melaksanakan tatacara ini dengan telus, ikhlas dan jitu mengikut prosedur yang telah ditetapkan.

Pengurusan aset alih kerajaan di dalam TD khasnya perlu diberikan perhatian yang sewajarnya oleh pihak-pihak yang telah dilantik dan dipertanggungjawabkan. Kerjasama daripada semua peringkat lapisan anggota dalam pasukan sehinggalah ke peringkat kementerian adalah merupakan kunci bagi mencapai kecemerlangan di dalam pengurusan aset alih kerajaan ini. Sikap adalah penentu utama kepada kejayaan setiap pekerjaan, betul sikap kita, sempurnalah setiap pekerjaan. Dengan perkembangan teknologi maklumat yang semakin berkesan, segala penyaluran maklumat akan lebih lancar dan seterusnya membantu pentadbiran di pasukan menjadi lebih mudah dan menjimatkan masa mahupun tenaga.

Tentera Darat perlu mempertingkatkan ilmu dengan memberi pendedahan yang lebih menyeluruh berkaitan tatacara Pengurusan Aset Alih Kerajaan ini kepada semua peringkat anggota di pasukan-pasukan dengan menganjurkan seminar, bengkel, syarahan ataupun hari pengajian.

Modul berkaitan Pengurusan Aset Alih Kerajaan ini juga perlu diwujudkan dan diperkenalkan di dalam silibus kursus-kursus melibatkan pengurusan stor pasukan yang dikendalikan di pusat-pusat latihan. Pengetahuan yang lebih mendalam juga perlu diberikan kepada semua jurulatih-jurulatih terlibat agar mampu dijadikan sebagai pakar rujuk kepada pasukan-pasukan dalam melaksanakan tatacara ini kelak.

Pemeriksaan dan pemantauan yang berterusan oleh Pegawai Atasan di setiap pasukan juga perlu dilaksanakan untuk menentukan pengisian setiap data kedalam rekod-rekod berkaitan aset-aset yang telah diterima sentiasa dikemaskini khasnya kepada aset-aset alih yang sentiasa bergerak bagi penempatan atau pinjaman sementara. Pemeriksaan yang dimaksudkan ini termasuk sama ada secara mengejut atau berkala. Dengan langkah ini, setiap pasukan akan mampu menghasilkan anggota-anggota yang terlibat di dalam pengurusan aset alih sentiasa berwaspada dengan mengemaskini data-data yang direkod kedalam borang-borang terlibat.

Di dalam proses penerimaan dan pendaftaran aset di pasukan, pegawai yang bertanggungjawab dilantik didalam pengurusan aset tersebut perlulah hadir bersama-sama anggota stor yang ditugaskan melaksanakan tugas penerimaan tersebut. Ini bagi memastikan segala data yang direkod pada permulaan kemasukan aset tersebut ke dalam perkhidmatan adalah lengkap dan mengikut prosedur pengisian sepertimana yang telah ditetapkan di dalam TPA. Sekiranya daripada permulaan lagi segala data yang direkodkan adalah lengkap, maka ianya tidak akan memberikan sebarang masalah yang sukar apabila aset tersebut telah sampai pada masa pelupusannya.

BIBLIOGRAFI:

1. Perintah Ulung Panglima Angkatan Tentera Ke-17.
2. Pekeliling Perbendaharaan Bil. 5 Tahun 2007.
3. Pekeliling Perbendaharaan Bil. 5 Tahun 2009.
4. Surat Pekeliling Perbendaharaan Bil. 12 Tahun 1995.
5. Surat Pekeliling Am Bil. 2 Tahun 1995.
6. Surat Arahan Perbendaharaan bertarikh 9 Mei 2008.
7. Surat Cawangan Logistik bertarikh 28 April 2008.
8. Surat Arahan Perbendaharaan bertarikh 24 September 2010.

Kapt Tengku Norazlinawaty binti Tuan Hamzah (3009549) telah ditauliahkan ke dalam Kor Ordnans Diraja pada 17 April 2004. Beliau pernah memegang jawatan Ketua KSOD di 42 WKSP RAD dan KSOD 51 WKSP RAD serta Pegawai Logistik Rej 881 PUTD. Beliau berkelulusan Diploma Pengurusan dari OUM-KTD. Beliau kini berkhidmat sebagai Ketua Sel Pakaian di 91 DPOD.

"....this is the group who leave not to escape from too much stress but to find greater sources of stimulation-and often greater remuneration for their intelligence and ability."

(Farber, 1991)

PENGENALAN

Fenomena *Burnout* masih merupakan satu perkara baru di Malaysia amnya dan di dalam Tentera Darat khasnya yang belum diberikan perhatian utama. Namun dengan beberapa insiden-insiden baru yang dialami di dalam Tentera Darat seperti peningkatannya kes-kes THTC, kes Bunuh Diri sejak kebelakangan ini telah membuka minda untuk mengkaji semula fenomena ini yang merupakan satu ancaman baru dalam dunia ketenteraan masa kini.

Fenomena *Burnout* ini telah lama dikaji di negara barat, secara umumnya ianya dikaitkan dengan tekanan yang dihadapi oleh seseorang sepertimana bebanan kerja yang banyak, kerja lebih masa dan pertembungan pendapat dengan majikan adalah merupakan sebahagian dari Burnout ini tetapi ini bukanlah faktor utama dalam Fenomena *Burnout*.

Konsep *Burnout* ini mula diperkenalkan oleh Freudenberger (1974) dengan mengemukakan isu sindrom Burnout di kalangan pekerja *front line human service* yang kurang terlatih dan selalu dibebani dengan kerja yang terlalu banyak.

DEFINASI

Sehingga kini masih tiada satu pengertian yang khusus tentang istilah *Burnout*. Secara umumnya istilah *Burnout* adalah berhubung rapat dengan tekanan namun Dr Herbert Freudenberger sebagai orang yang mula-mula mengkaji dan memperkenalkan Konsep *Burnout* telah megatakan kekosongan fizikal dan mental akibat situasi di tempat kerja[1]. Situasi di tempat kerja boleh dimaksudkan sebagai perkara-perkara yang berlaku melibatkan sesuatu perkerjaan manakala kekosongan yang dimaksudkan oleh beliau adalah penumpuan aspek kognitif dan tingkahlaku seolah-olah sudah tidak mempedulikan apa yang berlaku di sekeliling dan hanya melakukan kerja atas dasar terpaksa.

---

1. Norzihan Ayub, Ferlis Bahari dan Beddu Salam Baco, *Burnout* dan Komitmen Terhadap Organisasi di Kalangan Jururawat Hospital, Jurnal Kemanusian Bil 12, Dis 2008.

Menurut kamus psikologi Burnout bermaksud gangguan bagi individu yang terlibat dengan membantu orang. Kerjaya membantu orang ini amat meletihkan dan mengejar matlamat yang tidak mungkin dicapai sebagaimana yang diterangkan oleh Ellen L. Maher[2]. Ellen juga berpendapat kerjaya membantu yang dimaksudkan ialah kerjaya memberikan perkhidmatan yang memerlukan interaksi dengan pelbagai sikap orang ramai.

Burnout dan *Stress* adalah merupakan dua perkara yang berlainan namun saling berkait antara satu sama lain. Kesusahan yang dihadapi ketika menghadapi aktiviti-aktiviti harian dan ia boleh mengakibatkan *stress*. Antara kesusahan yang sering berlaku setiap hari ialah masalah kerja rumah, masalah masa, masalah persekitaran atau masalah kewangan. Kadangkala masalah yang berlaku dilihat sebagai perkara remeh tetapi apabila dibiarkan berlarutan, ia akan menjadi lebih serius. Perkara-perkara tersebut merupakan asas kepada terjadinya *stress*, iaitu kesukaran dalam melaksanakan tanggungjawab tertentu. Stress yang berterusan membawa kepada *Burnout*. Mengikut Greenberg dan Baron[3], *Burnout* menyebabkan ketandusan daya emosi (*emotional exhaustion*), ketandusan daya fizikal (*physical exhaustion*), penurunan sikap (*attitudinal exhaustion*) dan perasaan kurang pencapaian dalam kerjaya (*low feeling of accomplishment*).

Oleh itu *Burnout* boleh disimpulkan sebagai perasaan kegagalan, keletihan dan kelesuan yang ektrim akibat tuntutan yang terlalu membebankan ke atas tenaga, kekuatan atau kecekalan seseorang. Ianya didefinasikan sebagai pilihan terakhir (akibat) apabila satu siri percubaan untuk menangani tekanan yang dihadapi membawa hasil yang negatif dan gagal dalam mencapai kejayaan sebagaimana yang diterangkan oleh Farber[4].

HUBUNGAN TEKANAN DENGAN BURNOUT

Burnout lebih dilihat sebagai kemuncak kepada tekanan kerja di mana individu yang mengalami tekanan kerja yang berpanjangan dan tidak diuruskan dengan baik akan menghadapi *Burnout*. Mengikut Teori Super[5] yang diasaskan oleh Donald E.Super pula lebih dikenali menggunakan pendekatan proses, individu yang hampir kepada persaraan akan berkecenderungan untuk menghadapi *Burnout*. Ramai yang berpendapat pendekatan pemulihan perlulah ditangani di tahap tekanan lagi disebabkan

---

2. Ellen L. Maher, Burnout And Commitment: A Theoretical Alternative, The Personnel and Guidance Journal, Volume 61, Issue 7, March 1983.

3. Baron & Greenberg. 1995. Behavior in Organization Understanding and Managing The Human Side of Work. 5th Edition. USA: Prentice Hall.

4. Farber, B. A., Treatment strategies for different types of teacher burnout. Journal of Clinical Psychology, Volume 56, 1991

5. Super, D. E., A life-span, life-space approach to career development, Journal of Vocational Behavior, Volume 13, 1980.

apabila sudah *Burnout* mereka bagaikan sudah tidak mampu lagi membuat perubahan terhadap diri melainkan meninggalkan bidang pekerjaan mereka sekarang.

Tekanan kerja dan *Burnout* merupakan dua isu yang sangat penting khususnya bagi mereka yang terlibat dalam kerjaya membantu seperti Tentera, Jururawat, Guru, Pegawai Kebajikan dan sebagainya. *Burnout* ternyata berkaitan dengan tekanan kerja yang tidak dapat di atasi dalam satu jangka masa yang panjang sehingga melebihi tahap keupayaan individu itu untuk berhadapan dengan isu tersebut. Banyak kajian yang dijalankan menunjukkan bahawa mereka yang terlibat dengan profesyen membantu ini mudah mendapat *Burnout*. Sebagaimana yang dijelaskan pada bahagian pendahuluan iaitu tekanan adalah lebih memfokuskan aspek kognitif sahaja manakala *Burnout* memfokuskan kepada perkara-perkara seperti fizikal, intelektual, sosial dan psiko emosi seseorang itu.

Dari sudut fizikal kita dapat menenalpasti tanda-tanda *Burnout* apabila seseorang itu mengalami letih yang berpanjangan, penat, sakit-sakit biasa seperti sakit kepala dan mempunyai kesan sampingan kepada keseluruhan kesihatan untuk jangkamasa panjang. Tanda-tanda yang dimaksudkan lebih kepada perubahan yang dapat dilihat. Ianya akan kelihatan lebih jelas sekiranya seseorang yang menghadapi *Burnout* itu mungkin pada awalnya beliau adalah seorang yang sentiasa bertenaga dan bersemangat.

Dari sudut intelektual atau kebijaksanaan pula memfokuskan perubahan sikap tidak peduli kepada tugas yang diberikan dan mungkin juga kurang perhatian terhadap rakan-rakan sekerja. Individu yang terlibat juga mungkin bersikap kurang ambil berat terhadap keperluan keluarganya juga. Pendek kata mereka yang menghadapi Burnout menjadi malas untuk berfikir secara rasional kerana merasakan mereka berhadapan dengan tuntutan yang sangat tinggi dalam apa-apa juga perkara yang mereka lakukan.

Manakala dari segi sudut sosial pula membincangkan bagaimana individu yang menghadapi *Burnout* mula menunjukkan perubahan terhadap interaksi sosial mereka tidak kira di tempat kerja mahupun di rumah. Mereka mudah untuk bersikap biadab, cenderung untuk menggunakan bahasa kasar, tidak mahu berurusan dengan orang lain, sentiasa mengelak dari melakukan tugas-tugas penting dan suka menangguhkan kerja hingga saat-saat akhir.

Aspek emosi menyentuh tentang kognitif yang menjurus kepada terhasilnya perasaan bosan terhadap hidup, cenderung untuk mengasingkan diri, suka melupai perkara penting mungkin secara sengaja atau tidak sengaja dan ini mungkin berlaku disebabkan mereka sentiasa membayangkan tuntutan yang berlebihan kepada kerja-kerja yang dilakukan.

PUNCA-PUNCA *BURNOUT*

Punca-punca yang dikenalpasti yang boleh menyebabkan *Burnout* dapat diklasifikasikan kepada dua (2) sahaja iaitu diri sendiri dan persekitaran kerja. Setiap individu mempunyai banyak perbezaan dengan individu yang lain. Ini tidak dapat dinafikan kerana dari segi fizikal sahaja sudah cukup menunjukkan perbezaan kita. Apatah lagi jka kita menilai individu itu dari sudut keturunan, gaya hidup, pendidikan, penempatan bahkan taraf hidup juga amat menyumbang kepada perbezaan ini. Walau bagaimanapun amatlah jelas bahawa elemen diri sendiri ini sebenarnya berada di dalam kawalan individu itu sendiri. Dengan kata lain walaupun kita berbeza personaliti tetapi kita mampu bersaing dengan orang lain disebabkan faktor-faktor persaingan dan pembelajaran. Antara kelemahan individu yang dapat disenaraikan adalah seperti berikut:

1. **Kurang Ketahanan**. Setiap individu tidak mempunyai ketahanan yang sama dari segala sudut, contohnya ketahanan melawan penyakit. Hal ini dapat digambarkan sama dengan ketahanan setiap individu untuk menghadapi tekanan. Banyak faktor lain yang mempengaruhi ketahanan ini. Ia adalah berbentuk kognitif di mana ia biasanya terbentuk dari asuhan dan pengalaman yang dilalui. Hal ini juga bersangkut paut tentang bagaimana pendapat ahli psikologi Albert Ellis[6] (1957) yang menggambarkan bagaimana hidup manusia ini dipengaruhi oleh pemikiran yang tidak rasional. Ini secara tidak lansung amat menyumbang kepada ketahanan diri menghadapi tekanan. Kita patut tahu bahawa kita sebenarnya tidak diganggu dengan apa yang kita tempuhi sebaliknya kita diganggu oleh bagaimana kita mempersepsikan kejadian tersebut. Sebagai contoh seorang pekerja yang menerima surat teguran dari majikannya mungkin merasa tertekan sekiranya ia menganggap bahawa ia tidak sepatutnya diberi teguran seperti itu. Berbeza dengan individu lain yang menerima surat teguran yang sama yang menganggap bahawa itu adalah perkara biasa yang perlu dihadapi di dalam alam pekerjaan. Individu yang kurang ketahanan dalam menghadapi tekanan ini mungkin lebih banyak berfikir secara negatif dan sentiasa bersangka buruk kepada orang lain dan mungkin juga kepada diri sendiri.

2. **Kurang Kemahiran Mengurus Tekanan.** Kemahiran mengurus tekanan sepatutnya ada pada semua orang disebabkan orang lain tidak mendapat gambaran sebenar tentang apa masalah atau tekanan yang dihadapi oleh individu tersebut. Perkataan kemahiran merujuk kepada mahir yang membawa maksud individu itu mungkin tahu cara menguruskan tekanan tetapi kurang mahir. Cara mengurus tekanan ini juga didapati boleh terjadi banyak perbezaan di antara setiap individu disebabkan pengaruh agama, bangsa, gaya hidup dan mungkin juga jantina. Kadangkala sekatan ini juga harus dinilai dari segi keberkesanannya dan kemudaratan

6. Ellis, A., Rational Psychotherapy and Individual Psychology. Journal of Individual Psychology, Volume 13, 1957.

yang mungkin ada dengan cara yang kita lakukan. Ada individu yang merasa tenang apabila bersendirian, ada yang tenang bila dapat bersama keluarga dan sebagainya. Pendek kata individu itu sendiri harus tahu cara mengurus tekanan untuk dirinya sendiri dan beliau harus yakin akan keberkesanannya.

3. **Kelemahan Pengurusan Diri.** Pengurusan diri amat berkait rapat dengan faktor-faktor asuhan sejak dari kecil. Nilai-nilai keluarga yang dipentingkan perlulah dikenalpasti. Sesetengah individu tidak sedar bahawa kelemahannya dalam menguruskan diri mungkin menjadi penyebab kepada banyak tekanan yang bakal menimpa diri beliau. Antara kelemahan individu yang selalunya dikenalpasti adalah seperti berikut:

a. **Pengurusan Masa**. Kita perlu sedar bahawa setiap orang mempunyai peruntukkan masa yang sama banyak iaitu 24 jam sehari. Kelemahan dalam menguruskan masa ini kepada keperluan untuk diri sendri mampu membuatkan individu itu mengalami tekanan. Bagi individu yang tidak cekap menguruskan masa akan merasakan seolah-olah mereka tidak mempunyai masa yang cukup sedangkan masih banyak lagi perkara yang tidak diselesaikan. Ini boleh juga dipengaruhi oleh banyaknya komitmen yang perlu diberi. Secara sistematik seseorang itu perlu menilai diantara keperluan dan kehendak dalam memenuhi masanya.

b. **Keutamaan Kerja**. Keutamaan kerja dilihat dari segi kepentingan yang membawa maksud sejauh mana kemudaratan yang boleh berlaku sekiranya kerja itu tidak disiapkan. Tarikh akhir untuk menyiapkan tugasan yang diberikan juga menjadi faktor kepada keutamaan membuat kerja. Bagi seseorang yang tidak mahir menguruskan diri dari segi keutamaan kerja sentiasa menganggap bahawa semua kerja yang perlu diselesaikannya itu mempunyai darjah kepentingan yang sama. Ini akan menyebabkan beliau merasa bebanan tugas yang banyak yang dihadapi. Ini juga ada barsangkut paut dengan penurunan kuasa kepada staf bawahan seterusnya melibatkan kepercayaan kepada mereka. Kajian yang dilaksanakan oleh Norliana Mohd Bokri dan Mansor Abu Talib menunjukan julat bagi tekanan kerja iaitu mendapati julat skor adalah antara 7 hingga 25 (min = 17.00, sisihan piawai = 3.93) di mana 16 (13.3%) orang responden mengalami bebanan kerja yang rendah, seramai 88 (73.3%) orang mengalami bebanan kerja sederhana dan seramai 16 (13.3%) orang pula didapati mengalami bebanan kerja yang tinggi[7].

Manakala faktor persekitaran kerja menjadi punca seterusnya yang menyebabkan berlakunya tekanan. Namun seperti yang dijelaskan terdahulu bahawa persekitaran kerja ialah berada di luar kawalan setiap individu tetapi faktor inilah yang paling banyak

7. Norliana Mohd Bokti dan Mansor Abu Talib, Tekanan Kerja, Motivasi dan Kepuasan kerja Tentera Laut, Journal Kemanusian, Bilangan 15, Jun 2010.

mempengaruhi kepada punca-punca tekanan. Di sinilah wujudnya keperluan untuk berfikir secara positif. Ada pendapat mengatakan apabila anda bekerja maka anda sedang berhadapan dengan tekanan kerja. Ia bermaksud tekanan kerja adalah perkara yang tidak dapat dielakkan. Di sini juga kita membincangkan iaitu tekanan kerja ini tidak secara keseluruhannya berunsur negatif malah ia boleh menjadi sumber inspirasi kepada sesetengah orang. Antara faktor persekitaran kerja yang menyebabkan tekanan berlaku adalah:

1. **Masa Kerja Yang Panjang**. Ada masanya waktu kerja yang panjang tidak begitu mengganggu tetapi bagi mereka yang terlibat dengan tugas membantu dan tidak mendapat sebarang ganjaran daripada waktu kerja yang lebih itu akan menyebabkan seseorang itu akan menghadapi tekanan. Sekiranya ia berbentuk sekali-sekala sudah tentulah tidak menjadi hal tetapi sekiranya ia telah menjadi terlalu kerap sehingga mengganggu perjalanan hidup secara normal maka susahlah untuk individu itu menerima tekanan kerja ini secara positif.

2. **Kurang Masa Rehat.** Ada ketika pula waktu kerja nampak lebih terurus tetapi banyak komitmen yang terpaksa diberikan walaupun setelah tamat kerja akan turut memberi takanan kepada pekerja. Contohnya seseorang jururawat yang terpaksa berada dalam keadaan siap sedia atau on call, sudah tentulah mereka tidak dapat berehat dengan begitu selesa. Bahkan keadaan seperti ini lebih membuatkan pekerja merasa bahawa seolah-olah mereka dikongkong walaupun mereka tidak diberi apa-apa tugasan dalam tempoh masa tersebut.

3. **Kekaburan Peranan**. Ada beberapa bentuk penugasan yang kadangkala tidak begitu jelas dengan peranan mereka yang sebenarnya. Perkara ini akan menjadi bertambah rumit dengan pengurusan pihak majikan yang tidak begitu cekap dalam membahagikan tugas. Disebabkan keadaan seperti ini menyebabkan pekerja lebih bersifat mendiamkan diri dalam apa juga hal kerana ditakuti bahawa cadangan yang mereka berikan mungkin mereka sendiri yang terpaksa melakukannya. Jika mereka berada dalam keadaan tidak memahami peranan atau tugas mereka yang sebenar boleh menyebabkan tekanan kerana mereka merasakan tiada kepuasan terhadap kerja yang mereka lakukan di atas kaburnya matlamat dalam pekerjaan mereka.

4. **Banyak Peranan**. Terlalu banyak peranan sedikit berbeza daripada kekaburan peranan kerana ia lebih tertumpu kepada kerja yang bertimbun-timbun. Terlalu banyak tugas sehingga tidak mampu dilaksanakan oleh seseorang yang dianggap anyak peranan. Kayu pengukur yang dapat dilihat iaitu seseorang itu tidak dapat menyiapkan beberapa tugasan yang diberikan dalam tempoh masa yang ditetapkan dikira banyak peranan. Kes-kes begini banyak berlaku di jabatan-jabatan kerajaan di mana mereka terpaksa membuat kerja yang banyak disebabkan kekurangan pekerja.

5. **Monotoni**. Perkataan monotoni membawa maksud melakukan kerja yang berulang-ulang. Di dalam pekerjaan memanglah tidak dapat dielakkan daripada melakukan kerja yang sama tetapi melakukan kerja yang berulang-ulang tanpa diberi peluang untuk mencuba sesuatu yang baru akan mudah membuatkan pekerja merasa jemu. Majikan perlu bijak samada melakukan pusingan atau giliran tempat bertugas agar pekerja dapat merasakan peluang melakukan sesuatu kerja yang baru.Memang menjadi naluri manusia di mana kita suka menghadapi cabaran dan menimba pengalaman baru.

6. **Kurang kawalan.** Ada sesetengah pengurusan yang tidak begitu mementingkan kawalan dari segi pelaksanaan kerja ataupun displin. Ini bermakna tidak ada bezanya jika seseorang itu melakukan kerja dengan baik sekiranya kawalan kurang diberikan. Ini akan menyebabkan mereka membandingkan prestasi antara mereka. Perkara sebegini juga boleh mnyebabkan pekerja yang bersemangat akan turut menjadi lemah dan tidak produktif.

7. **Tiada Hubungan Baik Dengan Rakan Sekerja.** Manusia ini diciptakan untuk hidup bermasyarakat. Kalau dikaji semula sejarah perkembangan manusia tentang bagaimana sesuatu bangsa yang berjaya, mereka ini sebenarnya telah lama hidup secara bertamadun. Dari hidup yang bertamadun dan bermasyarakat inilah menjadikan manusia itu maju. Ini bermakna interaksi dengan rakan sekerja bukan sahaja menjadikan manusia dapat hidup dengan gembira tetapi kita boleh belajar perkara-perkara baru. Dengan adanya rakan baik di tempat kerja akan menjadikan kita juga berasa seronok untuk pergi ke tempat kerja. Selain daripada terikat dengan tugasan yang diberikan kita juga dapat bertukar-tukar fikiran tentang banyak perkara. Hubungan yang baik dengan rakan sekerja juga menjadikan mereka sebagai tempat untuk kita meluahkan masalah yang dihadapi.

8. **Tiada Sokongan**. Sokongan amatlah perlu kepada seseorang terutama di dalam melakukan kerjanya. Sokongan yang dimaksudkan adalah meliputi sokongan daripada majikan, rakan-rakan dan keluarga. Bentuk sokongan yang diterima mungkin berbeza tetapi setiap satunya mempunyai peranan yang juga berbeza. Misalnya sokongan daripada majikan mampu menjadikan seseorang itu ingin bersemangat untuk melaksanakan tugas. Antara bentuk sokongan daripada majikan ialah kenaikkan gaji, pujian dan anugerah khas. Manakala sokongan daripada rakan dan keluarga mampu untuk menjadikan seseorang itu untuk terus memajukan diri dalam apa juga bidang yang diceburi.

9. **Tiada Perkembangan Kerjaya.** Ada sesetengah pekerjaan yang kurang dari segi peningkatan atau perkembangan kerjaya. Kurang di sini membawa maksud kurang peluang ataupun tidak diberi peluang. Hal-hal sebegini perlu dititik beratkan kerana sesiapa sahaja yang menjadi pekerja sudah tentulah beliau amat berharapkan semoga kerja yang beliau lakukan menunjukkan perkembangan supaya beliau dapat berpuas hati dan berbangga terhadap pekerjaannya. Tidak ada manusia yang

mahu menjadi sepertimana beliau mula bekerja dan bersara semasa membuat kerja yang sama. Setidak-tidaknya mereka juga mahu menjadi seorang yang boleh memberi panduan kepada pekerja-pekerja baru. Ini akan berakhir dengan ketidakpuasan hati dalam pekerjaan. Contohnya dalam perkerjaan sebagai tentera, julat skor yang diperolehi dalam kajian oleh Norliana Mohd Bokti dan Mansor Abu Talib[8] juga mendapati seramai 30 (25.0%) orang berada di tahap berpuas hati. Sementara itu, 69 (57.5%) orang didapati berbelah bagi antara berpuas hati atau tidak berpuas hati dan hanya 21 (17.5%) orang sahaja didapati berasa tidak berpuas hati. Di dalam kajian ini, didapati 21 orang anggota tidak berpuas hati kerana tiada pekerbangan kerjaya yang mana ianya disebabkan oleh faktor lain seperti kegagalan anggota menghadiri kursus untuk kenaikan pangkat dan banyak lagi faktor penyumbang lain.

10. **Kurang Pengiktirafan**. Ada majikan yang merasakan ganjaran kewangan adalah yang terbaik dan dengan pemberian ganjaran mampu menaikkan semangat pekerja untuk terus setia di dalam pekerjaan. pemberian ganjaran secara umumnya dapat dibahagikan kepada dua jenis ganjaran yang utama iaitu ganjaran luaran (ekstrinsik) dan ganjaran dalaman (intrinsik). Ganjaran luaran membawa maksud ganjaran yang boleh dilihat dengan mata kasar seperti kenaikan gaji dan ia diletakkan sebagai sesuatu yang boleh dikawal manakala ganjaran dalaman adalah lebih kepada ganjaran yang tidak dapat dilihat dengan mata kasar seperti pujian yang mana ia diletakkan sebagai sesuatu yang di luar kawalan. Kedua-dua jenis ganjaran ini dilihat sebagai elemen penting yang banyak mempengaruhi pembentukan sikap seseorang itu yang boleh juga menjadi pembentukan sikap kepada keseluruhan organisasi. Melalui kajian ini juga didapati julat skor adalah antara 61 hingga 116 (min = 94.13, sisihan piawai 10.78) di mana seramai 18 (15.0%) orang bermotivasi rendah manakala 81 (67.5%) orang bermotivasi sederhana dan 21 (17.5%) orang bermotivasi tinggi.

LANGKAH-LANGKAH MENCEGAH *BURNOUT*

Seperti yang telah dikenalpasti bahawa *Burnout* adalah kemuncak kepada tekanan yang berpanjangan. Oleh itu pendekatan yang terbaik adalah dengan cara menguruskan tekanan itu terlebih dahulu. Antara pendekatan yang boleh dilakukan adalah melalui kaunseling. Pendekatan secara terperinci adalah seperti dari aspek kognitif dan aspek tingkahlaku setiap orang tersebut. Bagi aspek kognitif adalah berasaskan fikiran yang positif kerana sekiranya seseorang itu tidak berfikiran secara positif akan menyukarkan usaha-usaha yang bakal dijalankan. Antara usaha yang boleh dijalankan adalah seperti berikut:

1. **Hindari Tekanan Berterusan**. Perkara yang paling penting adalah untuk mengelakkan tekanan itu dihadapi secara berterusan tanpa mendapat cara

8. Norliana Mohd Bokti dan Mansor Abu Talib, Tekanan Kerja, Motivasi dan Kepuasan kerja Tentera Laut, Journal Kemanusian, Bilangan 15, Jun 2010.

menanganinya yang berkesan. Antara cara-cara menangani tekanan secara berterusan yang boleh dijadikan panduan adalah seperti berikut:

a. **Kenali Cara Sendiri**. Seseorang itu perlulah memahami kemampuan dan kebolehan diri sendiri. Mereka harus sedar bahawa setiap manusia adalah berbeza-beza. Kita tidak mampu mengikut cara orang lain kerana kita juga mempunyai cara kita sendiri. Kita harus yakin bahawa cara sendiri masih mampu mendapat pencapaian yang baik dalam melakukan kerja. Kita boleh meletakkan individu lain sebagai idola tetapi itu hanyalah sebagai panduan sahaja. Apa-apa yang kita lakukan atas kemampuan sendiri akan lebih memberi kayakinan kepada kita.

b. **Perubahan Sikap**. Membuat perubahan sikap yang lebih positif. Sentiasa menghormati dan menghargai orang lain agar kita dapat diterima dalam sesuatu kumpulan besar. Ini secara tidak lansung akan mengubah persepsi kita terhadap orang lain.

c. **Tidur Sebagai Pemusnah Tekanan Yang Hebat**. Ada sesetengah orang melihat tidur sebagai elemen yang tidak penting. Mereka tidak sedar bahawa tidur yang berkualiti merupakan suatu cara menangani *stress* yang sangat berkesan. Jadi cubalah untuk mendapat tidur yang berkualiti demi untuk merehatkan tubuh dan minda anda.

Manakala dari aspek tingkahlaku pula, adalah perlu cuba untuk buat perubahan terhadap perkara-perkara yang tidak digemari oleh orang lain. Ini adalah kerana tingkahlaku kita amat penting kepada orang lain. Kita tidak boleh memandang remeh teguran orang terhadap diri kita kerana kita mungkin tidak begitu jelas melihat keperibadian kita. Untuk mengubah tingkahlaku yang tidak diingini ini kita perlulah mendapat sokongan dari pelbagai pihak seperti berikut:

1. **Bina Ketahanan Diri**. Sokongan dari dalam diri merupakan asas yang kuat kepada perubahan tingkahlaku. Kita perlu membina ketahanan diri iaitu dengan cara melatih diri kita menerima tekanan dan kita kaji bagaimanakah untuk mengatasinya.

2. **Minta Nasihat Profesional**. Kita perlulah minta nasihat dari orang yang benar-benar layak memberi nasihat seperti majikan, orang yang telah berjaya ataupun dari rakan-rakan yang mampu membawa kita ke arah kebaikan.

3. **Rancang Hidup Anda**. Kita perlulah mempunyai perancangan dalam hidup. Setiap perancangan kita lakukan perlulah dikaji baik buruknya. Ini bermaksud kita tidak boleh *bias* dalam membuat perancangan hidup kita sendiri.

4. **Selesaikan Ikut Keutamaan**. Kita perlu bijak menilai pemberat kepada tugasan yang diberikan kepada kita kerana kita perlu tahu bahawa tidak semua kerja

mempunyai keutamaan atau kepentingan yang sama. Sekiranya ini tidak dititikberatkan maka ia akan membuatkan kita merasakan seolah-olah kita dibebani dengan tugas yang cukup banyak.

5. **Mempunyai Kehidupan Berkeluarga Yang Menyokong**. Kehidupan keluarga mampu menjadi sebagai ubat penenang kepada kita sekiranya kita mempunyai keluarga yang menyokong. Bagaimana untuk memiliki keluarga yang menyokong adalah dengan cara membuatkan mereka sedar bahawa kita bekerja untuk mereka dan sentiasa juga memberi keutamaan dalam masalah-masalah yang dihadapi oleh keluarga.

6. **Ceriakan *Mood***. Ceriakan *mood* anda terutama pada waktu-waktu yang anda rasa kurang bersemangat seperti mendengar muzik atau melakukan apa-apa sahaja yang boleh menceriakan anda. Dari itu cuba elakkan suasana yang boleh membuat anda menjadi negatif.

KESIMPULAN

Burnout adalah merupakan kemuncak kepada tekanan yang dialami secara berpanjangan. Fenomena ini sekiranya tidak dibendung akan mengakibatkan berlaku lagi kes-kes bunuh diri dan masalah sosial di dalam Angkatan Tentera.

Burnout menjurus kepada pembentukan tingkah-laku tidak peduli dan putus harapan di dalam pekerjaan. Kumpulan yang berisiko tinggi adalah mereka yang berkhidmat sebagai pekerja sosial yang terpaksa berhadapan dengan pelbagai karenah manusia. Keadaan ini akan membuatkan mereka berasa tidak puas dalam pekerjaan dan keletihan yang amat sangat. Burnout perlu ditangani bermula dari peringkat tekanan lagi. Perubahan-perubahan yang mampu dilakukan ialah dari aspek kognitif dan tingkahlaku. Selain individu organisasi juga perlu menitikberatkan tekanan yang dihadapi oleh pekerja-pekerja untuk mengelakkan *Burnout*.

Sewajarnya pihak Angkatan Tentera perlu memandang serius fenomena *Burnout* ini kerana tanpa kajian dan perhatian khusus, ini akan menjadi virus yang akan merebak dan menular di dalam setiap minda yang lemah.

BIBLIOGRAFI:

Journal

1. Baron & Greenberg. 1995. Behavior in Organization Understanding and Managing The Human Side of Work. 5th Edition. USA: Prentice Hall.
2. Ellis, A., Rational Psychotherapy and Individual Psychology. Journal of Individual Psychology, Volume 13, 1957.
3. Ellen L. Maher, Burnout And Commitment: A Theoretical Alternative, The Personnel and Guidance Journal, Volume 61, Issue 7, March 1983.
4. Farber, B. A., Treatment strategies for different types of teacher burnout. Journal of Clinical Psychology, Volume 56, 1991
5. Norliana Mohd Bokti dan Mansor Abu Talib, Tekanan Kerja, Motivasi dan Kepuasan kerja Tentera Laut, Journal Kemanusian, Bilangan 15, Jun 2010.
6. Norzihan Ayub, Ferlis Bahari dan Beddu Salam Baco, Burnout dan Komitmen Terhadap Organisasi di Kalangan Jururawat Hospital, Jurnal Kemanusian Bil 12, Dis 2008.
7. Super, D. E., A life-span, life-space approach to career development, Journal of Vocational Behavior, Volume 13, 1980.

Mej Mawarni binti Abdullah telah ditauliahkan ke dalam Kor Ordnans Diraja pada 11 Ogos 1997. Beliau pernah memegang berbagai jawatan penting di pasukan, Markas formasi, Markas Tentera Darat dan Markas Angkatan Tentera. Beliau berkelulusan Maktab Turus dan memiliki Diploma Pengurusan Perniagaan dari UiTM dan Diploma Eksekutif Pengajian Strategik dan Pertahanan dari UPNM. Beliau kini berkhidmat sebagai Pegawai Staf 2 Data Logistik, Bahagian Logistik Pertahanan, Markas Angkatan Tentera.

KESAN-KESAN KEBOCORAN MAKLUMAT KEPADA UMUM MELALUI PERKEMBANGAN TEKNOLOGI MAKLUMAT DAN LANGKAH-LANGKAH UNTUK MENGATASI MASALAH INI

oleh Koperal Norufendy bin Razali

Dalam pembangunan komunikasi yang melanda dunia tidak akan lengkap tanpa kewujudanperkembangan teknologi maklumat sebagai nadi utama perhubungan manusia. Tidak dinafikan bahawa terknologi maklumat memberikan bentuk baru pada corak kehidupan manusia. Penyebaran maklumat secara besar-besaran sudah tentu membawa kita menuju peradaban elektronik. Hal ini disebabkan teknologi komunikasi ini akan membawa kita kepada perkembangan yang berkaitan dengan pelbagai cara menerima dan menyampaikan maklumat seperti gambar, video, suara dan nombor yang diaplikasikan secara elektronik.

Oleh itu, teknologi maklumat menggabungkan komputer bersama teknologi komunikasi supaya dapat membentuk sistem-sistem bagi mengurus maklumat. Namun, sistem ini tidak terlepas daripada ancaman yang boleh mendatangkan impak buruk serta kesan negative kepada semua pihak. Ancaman yang dihadapi oleh pengguna teknologi maklumat datangnya daripada penggodam komputer, iaitu orang yang boleh mendatangkan ancaman kepada komputer dan sistem rangkaiannya. Mereka akan cuba menyalahgunakan kemudahan ini untuk kepentingan sendiri mahupun untuk organisasi tertentu. Namun begitu, terdapat golongan penggodam komputer yang menjalankan aktiviti khianat sebagai salah satu keseronokan semata-mata tanpa memikirkan kesan buruk yang akan menimpa pihak lain. Sebahagian penggodam komputer yang lain pula menjalankan aktiviti tersebut untuk menceroboh sistem rangkaian komputer dan mencuri data penting.

Selain itu, ada di kalangan mereka juga menghantar virus bagi mengganggu sistem rangkaian komputer hingga menyebabkan kerosakan serius. Tambahan pula, maklumat ialah bahan yang sangat berkuasa untuk menubuhkan atau menggulingkan sesebuah kerajaan dengan memperalat komputer dan rangkaiannya. Justeru itu, keselamatan pada zaman maklumat masih lagi diragui disebabkan wujudnya aktivis-aktivis tanpa sempadan ini yang dapat mengganggu sistem keselamatan dan turut memberi ancaman kepada negara.

Melalui peralihan teknologi ini banyak memberi kesan positif secara keseluruhannya, namun disebalik itu ada juga negatif ke atas perkhidmatan organisasi yang turut memberi impak besar kepada orang ramai. Dari sudut positif, antaranya pembayaran bil yang biasanya diuruskan di kaunter, kini diselesaikan di laman sesawang tanpa anda perlu keluar dari rumah. Malah lebih mudah lagi semua urusan juga turut dapat diselesaikan hanya melalui perisian yang terdapat di dalam telefon pintar. Negatifnya

pula, andaberhadapan dengan risiko maklumat diri yang terdedah kepada anasir jahat untuk dimanipulasi bagi mendapatkan keuntungan.

Justeru itu, pengguna juga perlu merasa sangsi dan bersedia dengan semua perubahan negatif yang terhasil akibat dalam era perubahan teknologi maklumat. Malah masih belum ada perisian keselamatan yang mampu menyekat sepenuhnya kecurian data dan perkongsian maklumat ini. Ia turut dikaitkan dengan perkembangan virus, malware, kod berniat jahat (*malicious*), bot jahat atau pelbagai jenis cecacing yang bertindak menggodam komputer untuk mencuri maklumat tanpa disedari oleh pihak pengguna. Kehilangan maklumat ini turut dikaitkan sebagai kebocoran data yang tidak diketahui pergerakannya.

Kecekapan penggodam ini memperolehi maklumat yang dikehendaki ini menyebabkan kebocoran atau ketirisan data yang diperolehi tidak disedari kehilangannya sama ada dimiliki oleh organisasi atau individu. Ia adalah masalah hari ini yang perlu diberi perhatian sepenuhnya kerana membabitkan kecurian maklumat yang dianggap sebagai hak peribadi individu atau organisasi. Kajian firma penyelidikan, InfoWatch meliputi negara di Asia Pasifik-Jepun dan Amerika Syarikat, mendapati punca kebocoran maklumat adalah berpunca dari perbuatan sabotaj yang kebanyakannya berpunca dari angkara pihak dalaman sendiri. InfoWatch mengesan 185 kebocoran data didaftarkan dalam pangkalan datanya sepanjang enam bulan pertama 2008.

Kehilangan data peribadi dianggap paling tinggi iaitu 95 peratus berbanding kebocoran data yang membabitkan rahsia komersial dan rahsia kerajaan. Ketirisan data pada 2008 tidak menampakkan sebarang perubahan berbanding tahun sebelumnya. Kehilangan komputer riba dan PDA berada di tangga teratas iaitu sebanyak 31 peratus berbanding kebocoran data menerusi Internet sebanyak 27 peratus. Pengarah Kanan Pemasaran Produk Symantec Corporation, Mathew Lodge berkata, berdasarkan Laporan Ancaman Keselamatan Internet Symantec XIII (ISTR XIII) bagi Julai hingga Disember 2007, Malaysia antara negara di Asia Tenggara yang menjadi tumpuan utama jenayah siber dengan berlakunya aktiviti penyebaran kod malicious berbanding negara lain iaitu sebanyak 68 peratus.

Selain itu, aktiviti pengiklanan, penukaran, penjualan dan pembelian maklumat pengguna seperti akaun bank, kad kredit, akaun eBay, PayPal dan kata laluan e-mel adalah salah satu tujuan penggodam untuk memecah masuk komputer pelayar dengan menggunakan perisian tertentu. Symantec turut melaporkan 499,811 maklumat dicuri dan dijual ke dalam pasaran gelap. Terdapat kes pekerja yang mengambil kesempatan dengan mencuri segala maklumat syarikat kemudian menjualkannya kepada syarikat pesaing demi memenuhi kehendak dan keuntungan kepada diri sendiri.

Ia membabitkan agensi kerajaan dan swasta yang tersohor di dunia seperti yang dihadapi oleh bank terkemuka Hong Kong yang berlaku tahun lepas dimana membabitkan sejumlah 159,000 transaksi data pemegang akaun dikatakan hilang daripada sistem

dengan keluarga, rakan dan rakan perniagaan. Kemudahan perkhidmatan melalui laman sesawang seperti *Facebook, Twitter* dan *Friendster* turut dapat meluaskan pengaruh, interaksi sosial dan kerjasama di antara pelbagai pihak.

Menurut Mathew, keselamatan maklumat bukan saja dengan cara memastikan ia terlindung daripada sebarang ancaman atau godaman luar malah turut memastikan maklumat itu tidak dicuri keluar dan disebarkan oleh mereka yang tidak bertanggung-jawab. "Organisasi perlu sentiasa melindungi dan menghadapi risiko kehilangan maklumat di samping mematuhi peraturan luar syarikat dengan dasar dalaman syarikat," katanya.

Menurutnya lagi, organisasi hari ini perlu memberi perhatian kepada Halangan Kehilangan Data (DLP) menerusi beberapa perkara iaitu perkembangan jaringan jalur lebar; tuntutan terhadap undang-undang negara dan Suruhanjaya Keselamatan memerangi jenayah kolar putih. Kes kecurian dan kehilangan data membabitkan badan kerajaan seperti pencerobohan sistem pangkalan data Perbadanan Tabung Pendidikan Tinggi Nasional (PTPTN) menggemparkan negara kerana dilihat sistem keselamatan agensi itu tidak kukuh hingga mampu dicerobohi penggodam.

Semua maklumat peminjam yang keseluruhannya merupakan penuntut institusi pengajian tinggi (IPT), dipadam terus daripada pangkalan data PTPTN oleh penggodam. Malahan sindiket yang didalangi penggodam komputer tersebut juga cuba membuat keuntungan melalui iklan khidmat yang menyediakan perkhidmatan melupuskan data peminjam dengan mengenakan caj yang tinggi sebanyak RM2,000 seorang ini didakwa mampu menghapuskan data pinjaman sekali gus membebaskan individu itu daripada membayar balik pinjaman yang telah dibuat. Salin itu, perkara yang serupa turut dikesan dimana penggodam menceroboh Sistem Pendaftaran Tanah Berkomputer Pejabat Tanah dan Galian (PTG) di beberapa negeri termasuk Wilayah Persekutuan Kuala Lumpur yang dikatakan menggunakan 'orang dalam' yang bertujuan memalsukan geran tanah bagi kawasan yang dikehendaki oleh pelanggannya. Hal ini adalah jenayah yang sangat merugikan pihak yang terbabit dan boleh menyebabkan kecelaruan terhadap data dan maklumat yang digodam.

Menurut Ketua Pegawai Eksekutif CyberSecurity Malaysia pula, berdasarkan analisis kecurian data berlaku kepada organisasi atau individu yang dikenalpasti mempunyai maklumat penting dan kebiasaannya membabitkan ancaman dalaman. "Dari Januari hingga September 2008, sebanyak 1,346 insiden dilaporkan, termasuk 471 insiden pencerobohan siber dan 55 insiden ancaman godama n (hack threat). Bagi 2007, sejumlah 1,038 insiden siber telah dikendalikan berbanding 1,372 insiden pada tahun 2006," katanya. Kebanyakan organisasi tidak mempunyai polisi yang lengkap untuk memelihara maklumat daripada diakses mereka yang tidak diberi kuasa. Oleh itu, organisasi sedemikian dinasihatkan agar mengetat dan meningkatkan kawalan keselamatan pentadbiran dengan menyatukan pentadbiran korporat agar jenayah seperti ini dapat dibendung.

Setiap organisasi seharusnya memiliki polisi maklumat keselamatan dan mentakrif polisi dokumen terhadap semua data dan maklumat yang terdapat di dalam simpanan pangkalan data mereka. Perkara ini dapat dilaksanakan bermula dengan penilaian terhadap kandungan maklumat, ancaman dan kemusnahannya di bawah kawalan pengurusan atasan. Katanya lagi, kehilangan data boleh berlaku disebabkan beberapa aspek kelemahan iaitu secara teknikal, fizikal dan sosial.

Serangan terhadap komputer boleh menjadikan sesebuah organisasi lumpuh dalam menjalankan perkhidmatan mereka lebih-lebih lagi seandainya tidak mempunyai sebarang pelan sokongan (*back up- plan*) untuk menangani permasalahan tersebut. Tahap keyakinan pengguna pula pasti merosot. Kebocoran maklumat sulit sesebuah organisasi akan menyebabkan strategi pemasaran dan persaingan diketahui oleh pihak lawan dan menjurus kepada kejatuhan organisasi tersebut.

Bagi mengatasi jenayah ini, adalah sangat penting bagi organisasi untuk membangunkan dasar keselamatan maklumat dan disokong oleh prosedur yang bersesuaian. Berdasarkan kepada standard antarabangsa Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001:2005, terdapat sekurang-kurangnya dua kawalan yang boleh dilaksanakan untuk mengawal keselamatan maklumat dalam sesebuah organisasi iaitu klasifikasi maklumat adalah perlu apabila ia perlu dipertingkatkan berdasarkan nilai, keperluan undang-undang, sensitiviti dan kepentingan maklumat tersebut.

Selain itu, maklumat juga perlu dilabelkan mengikut klasifikasi yang ditentukan mengikut tahap kerahsiaannya. Seterusnya, pengendalian maklumat secara sistematik haruslah dilaksanakan dengan menggunakan prosedur yang ketat.

CyberSecurity Malaysia turut menggariskan beberapa panduan keselamatan kepada individu dan organisasi bagi mengelakkan sebarang penipuan internet seperti seseorang individu perlulah berhati-hati ketika memberi maklumat peribadi di dalam laman web, e-mel, sistem pesanan segera, bilik bual atau pada papan mesej, terutamanya apabila diterima daripada pihak yang tidak dikenalpasti. Individu berhak bertanya mengapa dan bagaimana maklumat itu mahu digunakan oleh pihak terbabit. Individu juga perlu melindungi maklumat peribadi kerana ia merupakan maklumat yang amat berharga.

Malah, kita juga harus mengenalpasti siapa pihak yang kita selalu berurusan. Penggunaan perisian seperti anti virus, anti *spyware* dan *firewall* adalah penting bagi memastikan data sentiasa dikemas kini. Sistem operasi dan penyemak imbas laman web perlu ditetapkan dan dikonfigurasikan dengan betul dan mengikut langkah-langkah yang telah ditetapkan. Kita juga perlu melindungi kata laluan komputer, e-mel dan laman penting dengan menggunakan gabungan huruf, symbol dan nombor. Malah, fail yang penting juga perlu dibuat sandaran bagi memastikan segala data-data tidak hilang dan masih mempunyai *'back-up'* data jika data tersebut telah digodam.

Selain itu, pengurusan keselamatan dalam organisasi hendaklah membuat jadual bagi data sandaran pada kekerapan yang boleh diharapkan. Selain itu, mengekalkan data sandaran dalam tempoh tertentu untuk membenarkan pemulihan semula atau isu pembaikan yang tidak didedahkan serta-merta. Pengguna juga boleh menggunakan sandaran secara automatik dan melakukan siri ujian kepada proses penyalinan. Pejabat juga hendaklah menyediakan komputer tambahan untuk sentiasa menyalin data serta memastikan data sandaran mempunyai log tarikh dan masa supaya dapat disahkan. Selain dari itu, dengan membuat sandaran untuk pelbagai jenis medium seperti salinan cakera mudah alih, CD, dan *'harddisk*' ini turut dapat membantu agar data–data asal tidak boleh diubahsuai dan meletakkan data sandaran tersebut di tempat yang selamat.

Bagi memastikan keberkesanannya juga, penggunaan e-mel hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet. Di antara prosedur-prosedur pengurusan e-mel adalah menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel bombing. Penghantaran dokumen rasmi juga hendaklah menggunakan e-mel rasmi jabatan sahaja dan pentadbir e-mel perlu menetapkan had minimum kuota mailbox. Pembersihan e-mel hendaklah dibuat sekiranya mailbox didapati tidak aktif selama dua bulan atau melebihi kuota dan had masa yang ditetapkan.

Langkah lain yang boleh dilakukan ialah menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi Universal Resource Location (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan. E-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang bersesuaian.

Disamping itu, polisi, prosedur kawalan penghantaran dan penerimaan maklumat yang formal perlu diwujudkan untuk melindungi maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi melaui perjanjian perlu diwujudkan untuk penghantaran dan penerimaan maklumat di antara jabatan dengan pihak luar. Medium yang mengandungi maklumat penting serta penyalahgunaan atau kerosakan semasa pemindahan dan penerimaan maklumat yang terdapat dalam mel elektronik dan perlu dilindungi daripada capaian yang tidak dibenarkan. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat jabatan.

Bagi perlindungan data atau keselamatan teknologi maklumat, ia perlu dilaksanakan secara proaktif iaitu perlu ada perancangan dalam melaksanakan kaedah-kaedah pencegahan keselamatan teknologi maklumat ini. Satu masalah dalam perkara ini adalah ia memerlukan modal yang tinggi dan tenaga kerja yang mahir. Hasilnya jua agak sukar untuk dijangkakan atau ditunjukkan kepada pihak pengurusan melainkan sehinggalah berlakunya pencerobohan data atau maklumat tersebut. Di sini, pihak teknologi maklumat perlu bijaksana dalam membentang perancangan tersebut berserta

dengan angka-angka pulangan pelaburan kepada syarikat.

Ini kerana kos untuk mengembalikan data atau maklumat yang telah hilang atau rosak adalah sangat tinggi berbanding dengan kos pelaburan untuk pencegahan pencerobohan keselamatan teknologi maklumat. Ia perlu dianalisis dan dibuat perbandingan dengan lebih teliti.

Kesimpulannya, secara umumnya penulis nyatakan di sini perlu ada tiga perkara paling asas dalam perlaksanaan pencegahan pencerobohan keselamatan teknologi maklumat ini iaitu merangkumi faktor-faktor perimeter keselamatan, pendidikan dan polisi. Faktor perimeter keselamatan merupakan alat-alat dan teknik-teknik keselamatan yang perlu ada dalam sistem keselamatan teknologi maklumat seperti penggunaan *Firewall, Intrusion Detection System, Intrusion Prevention System,* perisian antivirus, teknik DMZ (Demilitirized Zone) dan sebagainya.

Di sebalik itu, tenaga kerja yang pakar dan terlatih diperlukan untuk mengurus dan mengendalikan dengan baik perimeter-perimeter keselamatan teknologi maklumat ini. Satu sistem keselamatan teknologi maklumat yang menyeluruh perlu dilaksanakan ke atas kesemua infrastruktur dan kemudahan teknologi maklumat yang ada dalam sesebuah syarikat atau organisasi. Kemudian, faktor pendidikan iaitu kesemua para pekerja dan pelanggan yang terlibat dengan penggunaan komputer dan sistem maklumat bagi sesebuah syarikat, perlu dididik dengan betul untuk menggunakannya dengan bijaksana dan selamat.

Ini penting kerana dengan sistem perimeter keselamatan yang canggih belum tentu ia terjamin dapat melindungi keselamatan sesebuah maklumat atau data. Sebagai contoh, apabila berlaku pencerobohan sesuatu akaun bank pengguna di internet, pihak bank menyatakan mereka mempunyai sistem keselamatan yang kukuh dan menyalahkan pihak pengguna yang tidak mengendalikan dengan betul penggunaan akaun bank mereka. Walhal ironinya, pengguna akaun bank tersebut tidak dididik dengan betul dan bijaksana oleh pihak bank terbabit. Mereka hanya mempromosi dengan gigih berkenaan dengan perbankan internet kepada pengguna tetapi tidak tahu bagaimana untuk menggunakan perbankan internet secara bijaksana dan selamat.

Pengguna dan pelanggan yang tidak dapat menggunakan infrastruktur teknologi maklumat dengan betul dan selamat akan menjadi sasaran kepada pihak penceroboh dengan pelbagai teknik penipuan seperti kejuruteraan sosial, phising, fraud dan sebagainya. Jabatan Teknologi Maklumat perlu membuat banyak kempen kesedaran dengan menyediakan poster-poster panduan keselamatan siber dan sebagainya seperti apa yang dilakukan oleh pihak CyberSecurity Malaysia ketika ini untuk kempen penggunaan Internet yang selamat di kalangan rakyat di Malaysia. Pihak syarikat atau organisasi juga boleh berkerjasama dengan pihak CyberSecurity Malaysia untuk mendapatkan info yang lebih mendalam mengenai hal ini.

Seterusnya adalah faktor polisi iaitu apa yang boleh dibuat dan apa yang tidak boleh dibuat oleh seseorang dalam mengendalikan sesuatu infrastruktur dan perkhidmatan teknologi maklumat bagi sesebuah syarikat atau organisasi. Setiap penggunaan perkhidmatan teknologi maklumat seperti komputer, Internet, sistem maklumat, rangkaian komputer dan sebagainya perlu ada polisi keselamatan tersendiri di samping polisi keselamatan teknologi maklumat yang umum. Ia merupakan faktor kawalan yang penting terhadap pengunaan kemudahan teknologi maklumat bagi sesebuah syarikat atau organisasi. Sekiranya berlaku sesuatu yang tidak diingini, ada polisi keselamatan yang akan cuba mengimbanginya. Sebagai contoh, para pekerja tidak dibenarkan melayari laman web lucah, laman web sosial dan sebagainya pada masa bekerja.

Sekiranya berlaku, ada tindakan susulan yang akan dikenakan kepada para pekerja terbabit oleh pihak syarikat seperti penggantungan kerja, denda dan sebagainya. Kunci utama bagi perlindungan data pengguna bagi sesebuah syarikat adalah perlu diketahui berkenaan dengan di mana dan bagaimana data itu disimpan, siapa yang boleh mencapainya, bagaimana untuk melindungi data tersebut daripada dicuri, disebar dan dikongsi di kalangan penyangak teknologi. Kesedaran dan tindakan yang agresif daripada pelbagai pihak adalah sangat perlu bagi membendung kebocoran maklumat menerusi perkembangan teknologi maklumat.

BIBLIOGRAFI:

Buku:

1. Konflik dan Kesamaran Peranan di Kalangan Personel Teknologi Maklumat (IT) di Sektor Awam di Malaysia. Utusan Publications & Distributions Sdn.Bhd Kuala Lumpur,1990. Mashitah Abdul Manan, Zawiyah Mohammad Yusof, Ibrahim Mohamed & Kamaruzzaman Matharsha. 344 muka surat.
2. Industri Tenaga Kerja Teknologi Maklumat dan Komunikasi di Malaysia. Petaling Jaya Prentice Hall Pearson Education Malaysia Sdn Bhd, 2000 .Nur Atiqah Abdullah, Ahmad Khairy Ahmad Domil & Nik Mutasim Hj. Nik Abd. Rahman. 211 muka surat.

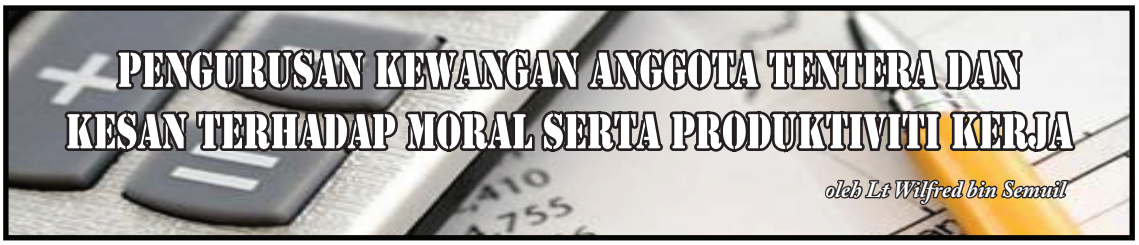
Artikel Akhbar/ Buletin:

1. Atikah Ali. Selamatkah Maklumat Anda. Harian Metro 5 November 2008. Muka surat 5

Laman Web:

1. Kelemahan Teknologi Maklumat. www.mindasasterabahasa.com 28 Julai 2011
2. Cybersecurity Bantu Cegah Jenayah Siber. www.cybersecurity.org.my 16 Ogos 2007

1150979 Kpl Norafendy bin Razali mulai memasuki tentera seawal usia 22 tahun telah menamatkan Latihan Perajurit Muda pada 24 Jun 2005 seterusnya beliau diserap ke dalam Kor Perkhidmatan Diraja dalam Tred Pemandu. Beliau sebelum ini telah terlibat dalam sukan JUDO ATM di Pengkalan TLDM Lumut, Perak dan sekarang ini beliau berkhidmat di pasukan Markas Garison Terendak sebagai Penolong Ketua Seksyen di Cawangan Kenderaan.



PENGURUSAN KEWANGAN ANGGOTA TENTERA DAN KESAN TERHADAP MORAL SERTA PRODUKTIVITI KERJA

oleh Lt Wilfred bin Semuil

PENDAHULUAN

Pengurusan kewangan adalah satu proses dan strategi perancangan yang dirangka dengan baik yang menggunakan sumber kewangan yang diperolehi untuk mencapai matlamat jangka masa sederhana dan panjang. Pada masa kini kebanyakan anggota tentera mempunyai masalah kewangan untuk sara diri dan keluarga. Perkara ini jika dibiarkan berterusan akan menyebabkan prestasi kerja anggota akan menurun serta akan berlakunya masalah disiplin. Perkara ini adalah disebabkan pengurusan perbelanjaan anggota itu sendiri yang tidak di kawal dengan berhemah. Pengurusan kewangan adalah segala yang berkaitan dengan mengurus kedudukan ekonomi atau kewangan seseorang individu dengan mengambil kira perkara-perkara yang ingin dilakukan seperti berkahwin, membeli harta seperti kereta atau rumah, merancang untuk mendapatkan anak serta perancangan pendidikan anak. Melalui perancangan kewangan, kita dapat mengenal pasti cara-cara membuat belanjawan, menabung dan membelanjakan wang dalam suatu tempoh masa yang tertentu. Selain itu juga, ia adalah panduan untuk membantu kita mencapai sesuatu matlamat pada masa hadapan. Menerusi perancangan kewangan ini kita dapat melihat di manakah kedudukan kewangan peribadi pada masa kini, halatuju pada masa depan, bagaimana untuk mencapainya dan bila sepatutnya bermula.

Kita sering kali terdengar tentang kisah wang dan masalah-masalah yang dihadapi disebabkan oleh kegagalan pengurusan wang. Namun begitu pernahkah kita terfikir apakah punca kepada semua permasalahan yang timbul itu. Jika kita renungkan kembali, kitalah yang menentukan sama ada wang dapat memberi keselesaan atau pun kesengsaraan kepada diri kita sendiri. Kita perlu tahu cara atau amalan yang betul dalam menguruskan kewangan peribadi supaya masalah ini tidak akan timbul. Konsep pengurusan kewangan peribadi itu sendiri sebenarnya amat ringkas iaitu perbelanjaan tidak sepatutnya melebihi pendapatan dan simpanan perlu ditetapkan sebelum membuat perbelanjaan. Namun sejauh mana konsep ringkas ini dapat diikuti, itulah yang menjadi persoalan sehingga kini. Tidak dinafikan wang merupakan medium yang sangat penting dalam kehidupan seharian kita. Namun kita sebagai manusia sering kali melakukan kesilapan dalam menguruskan wang sehinggakan ia bukan sahaja menghantui golongan berpendapatan rendah, malahan yang berpendapatan agak lumayan juga tidak dapat lari dari masalah pengurusan kewangan.

PUNCA UTAMA MASALAH PENGURUSAN KEWANGAN

Tidak Mempunyai Simpanan Kecemasan

Antara punca masalah kewangan adalah tidak mempunyai simpanan kecemasan. Perkara ini penting dalam kehidupan kerana, kita tidak dapat menjangkakan apa yang akan berlaku pada masa hadapan sekiranya kita ataupun ahli keluarga ditimpa penyakit atau kemalangan. Namun, sekiranya kita mempunyai simpanan khas untuk perkara kecemasan, sekurang-kurangnya bebanan yang ditanggung tidaklah terlalu berat. Ia juga dapat memberi ruang dan pilihan untuk kita memikirkan tindakan terbaik yang kita perlu lakukan. Satu cara yang terbaik ialah dengan membeli insurans kesihatan. Ramai orang yang kurang peka terhadap kepentingan insurans kesihatan ini. Insurans kesihatan bukan sahaja dapat membayar bil-bil perubatan dan pembedahan, malah anggota juga boleh menggunakannya untuk menolak cukai tahunan daripada Lembaga Hasil Dalam Negeri (LHDN).

Tidak Dapat Membezakan Antara Keinginan Dan Keperluan

Seterusnya ialah tidak dapat membezakan antara keinginan dan keperluan. Ini juga satu punca utama yang menyebabkan anggota tentera mengalami masalah kewangan. Boleh dikatakan lebih 60% pembeli menyatakan bahawa mereka membeli mengikut keinginan dan bukannya keperluan. Kita perlu bijak dalam merancang perbelanjaan supaya ia tidak akan memudaratkan diri sendiri pada masa hadapan. Keperluan ialah sebarang benda yang betul-betul perlukan untuk memastikan matlamat tugasan anda tercapai. Contohnya seperti komputer riba bagi seorang anggota amat penting untuk memastikan semua tugasan yang diberikan dapat dilaksanakan dengan baik dan dihantar mengikut masa yang telah ditetapkan. Keinginan ialah benda-benda yang tanpanya anda masih boleh membuat kerja dan meneruskan hidup seperti biasa. Contohnya, membeli sesuatu kerana mementingkan jenama, sedangkan masih ada produk yang mampu milik, berkualiti dan mampu membantu anda untuk mencapai sesuatu objektif. Istilah 'biar papa asal bergaya' tidak seharusnya diguna pakai.

Masalah Sosial

Masalah sosial juga menjadi punca kepada masalah kewangan kepada kita, antaranya seperti yang sering berlaku terhadap anggota tentera darat tidak kira sama ada anggota lain-lain pangkat mahupun pegawai ialah terjebak dalam perjudian, dadah serta pusat-pusat hiburan seperti rumah urut dan kelab-kelab malam. Sebagai contoh, Perjudian akan memudaratkan diri serta kewangan keluarga kerana kebanyakan ianya berlaku apabila kalah dalam perjudian dan individu akan mencari jalan mudah bagi mendapatkan semula wang, dengan mengambil jalan mudah iaitu meminjam wang dari agensi yang tidak berlesen. Ini bukan sahaja menyebabkan masalah kewangan tetapi juga akan memberi masalah kepada ahli keluarga sekiranya anggota tidak dapat melangsaikan hutang mereka kerana terpaksa membayar hutang dengan faedah yang

tinggi. Penglibatan diri dalam aktiviti kelab malam serta aktiviti pelacuran di pusat rumah urut juga adalah pendorong kepada masalah kewangan sehingga sanggup membelanjakan wang yang banyak semata-mata untuk menikmati keseronokan.

Peningkatan Kos Sara Hidup

Peningkatan kos sara hidup seperti kenaikan harga barang dan perkhidmatan di kawasan bandar mendatangkan masalah bagi anggota tentera yang tinggal di bandar terutama di Kuala Lumpur berbanding dengan anggota yang tinggal di kawasan luar bandar. Jumlah pendapatan bersih anggota yang terhad menyebabkan kuasa beli anggota tentera yang di kawasan bandar adalah kecil dan secara tidak langsung mendorong mereka untuk membuat pembelian secara kredit. Peningkatan taraf hidup menyebabkan perubahan iaitu sebagai contoh, dahulu telefon bimbit dan komputer riba adalah kehendak tetapi disebabkan peningkatan taraf hidup maka ianya telah menjadi keperluan kepada setiap orang. Adakah punca masalah yang sering dilakukan ini tiada penyelesaiannya? Berdasarkan pengalaman dan pemerhatian yang dibuat, terdapat beberapa kaedah yang boleh dijadikan panduan dalam menguruskan kewangan peribadi dan sepatutnya diamalkan dalam menguruskan kewangan.

CARA MENGATASI MASALAH KEWANGAN

Membuat Anggaran Perbelanjaan

Kita bebas membuat pilihan dan keputusan mengenai kewangan agar tidak terikat dengan bebanan hutang, kuasa beli, liabiliti jangka panjang dan psikologi krisis kewangan. Sedarkah kita bahawa, walaupun kita mempunyai kebebasan dalam kewangan, namun kita juga memerlukan perancangan kewangan yang betul. Terdapat dua asas penggunaan wang iaitu guna dan simpan. Walaupun ada anggota tentera yang berjimat cermat namun, individu tersebut tetap akan menghabiskan sebahagian besar pendapatannya. Bagi seorang Pegawai muda tentera, mereka seharusnya peka terhadap pengurusan kewangan kerana ada dikalangan mereka kerap berbelanja di tempat seperti kelab malam yang mana seperti yang diketahui umum, harga minuman keras di kelab malam adalah mencecah RM 400.00. Perkara ini juga melibatkan anggota lain-lain pangkat dan mereka haruslah membelanjakan wang dengan berhemat dan buatlah keputusan bijak terhadap rancangan kewangan serta elakkan belanja secara boros. Anggaran perbelanjaan adalah kunci untuk mengawal pengaliran wang dan tujuan perbelanjaan dibuat. Jika anggaran perbelanjaan tidak mencerminkan kehidupan yang baik maka individu haruslah segera sedar bagi mengelakkan penyesalan dikemudian hari.

Mengurus Perbelanjaan Kredit Dengan Betul

Kredit adalah bidang kewangan peribadi yang menyebabkan ramai anggota tentera terjebak dalam masalah kewangan. Kredit membolehkan seseorang untuk menerima wang, barang, atau perkhidmatan dalam bentuk pinjaman dengan bersetuju untuk

membayar pinjaman pada jangka waktu dan kadar bunga kredit tertentu. Pemantauan daripada pegawai atasan adalah satu cara untuk mengawal pengurusan kredit bagi anggota yang baru atau yang telah lama terjerumus kepada pengurusan kredit yang tidak betul. Pengurusan kredit yang betul adalah tentang kefahaman tentang pinjaman wang bagi mendapat tawaran yang baik dan bagaimana untuk mengira beban kewangan dan bayaran bulanan. Ia juga melibatkan bagaimana untuk memperbaiki catatan kredit yang buruk dan tempat untuk mendapatkan bantuan jika anda mendapat kesulitan. Tidak dapat dinafikan anggota tentera mudah untuk mendapatkan pinjaman di koperasi tentera dan wujudnya kerjasama daripada agensi pusat pinjaman dengan Pegawai Memerintah adalah suatu usaha untuk membendung anggota daripada membuat pinjaman yang berlebihan. Setiap anggota harus melatih diri atau hak sebagai pengguna untuk memilih atau menolak pelbagai produk dan perkhidmatan yang tidak berkepentingan dan jangan mensia-siakan pendapatan yang telah diperolehi.

Pengurusan Insurans

Walaupun betapa berhati-hatinya dalam menjalani kehidupan, anggota tentera tidak boleh mengelak daripada berdepan dengan kemalangan. Keperluan insurans untuk melindungi diri dan harta peribadi daripada kemalangan, kesakitan, kecacatan, atau kematian. Anggota tentera sememangnya mempunyai perlindungan insurans khusus iaitu insurans kelompok namun pegawai ataupun anggota juga digalakkan untuk mendapatkan perlindungan insurans selain insurans tersebut. Antara tujuannya adalah untuk melindungi pendapatan keluarga. Bagi kebanyakan keluarga, kesinambungan pendapatan adalah bergantung kepada kehidupan dan kesihatan pencari nafkah. Insurans hayat yang secukupnya dapat menjamin pendapatan keluarga dalam apa jua keadaan. Seterunya ialah perlindungan kewangan sekiranya anggota ataupun pasangannya hilang upaya, maka insurans hayat akan memastikan keperluan keluarga tidak terjejas. Selain daripada itu insurans juga merupakan pelan untuk pendidikan anak-anak. Semua ibu bapa mempunyai impian yang tinggi terhadap masa depan anak-anak mereka justeru insurans hayat mampu menjadikan impian itu suatu kenyataan. Insurans juga merupakan salah satu medium tabung persaraan. Anggota yang bekerja mengharapkan suatu persaraan yang membahagiakan dan insurans hayat adalah langkah praktikal ke arah matlamat tersebut.

Rancangan Masa Hadapan

Merancang untuk masa hadapan seperti tahun persaraan, dan bakal pewaris kepada harta individu adalah penting melalui perancangan kewangan seperti pembelian tanah adalah relevan untuk setiap lapisan anggota tentera. Semasa menyediakan matlamat dan rancangan kewangan, individu perlu menimbangkan impak daripada faktor sampingan seperti cukai dan kadar faedah bagi pilihan agensi kewangan. Perubahan sampingan dalam persekitaran dan keadaan lain boleh merubah perancangan kewangan walaupun matlamat individu tidak berubah. Secara umumnya, dua faktor sampingan utama yang berkaitan dengan perancangan kewangan peribadi

adalah polisi kerajaan dan situasi ekonomi umum. Menyedari pentingnya perancangan kewangan, anggota tentera hendaklah sentiasa berhati-hati dalam perbelanjaan. Setiap individu perlu merancang kewangan agar tidak terjerumus dengan hutang. Ini melibatkan jaminan masa depan kerana pelbagai kemungkinan boleh berlaku sama ada baik atau buruk, kedua-duanya memerlukan aktiviti pengaliran wang keluar masuk. Sedarlah bahawa setiap perubahan dan tindakan bermula daripada diri sendiri.

KESAN TERHADAP MORAL DAN PRODUKTIVITI

Dalam konteks perkhidmatan Angkatan Tentera Malaysia (ATM), pengurusan kewangan yang lemah akan memberi implikasi negatif kepada moral dan produktiviti pegawai dan anggota tentera. Definisi moral dari segi ketenteraan meliputi bidang yang luas iaitu dari aspek daya juang, motivasi, kepimpinan, setiakawan, kejujuran, amanah, kesetiaan, kerohanian dan seumpamanya. Manakala produk yang ditawarkan oleh ATM adalah perlindungan kepada keselamatan kedaulatan Negara daripada ancaman dalam dan luar Negara. Produktiviti ATM pula merujuk kepada kecekapan dan keberkesanan organisasi ini dalam menguruskan soal keselamatan Negara. Berdasarkan kepada definisi-definisi diatas dapat dirumuskan bahawa konsep pengurusan kewangan memberi kesan secara langsung kepada moral dan produktiviti ATM dalam memberikan perkhidmatan yang terbaik kepada Negara dan masyarakat.

Anggota ATM yang mempunyai masalah akibat pengurusan kewangan yang lemah akan membawa kesan kepada moral dari sudut motivasi. Kesan terhadap motivasi ialah anggota tentera tidak akan mempunyai semangat untuk bekerja. Anggota yang bermasalah boleh menjadi sensitif, malu ataupun bersikap agresif serta sering berasa terlalu bimbang terhadap kerjaya malah perkara ini akan mengganggu prestasi di tempat kerja dan menyebabkan penurunan produktiviti. Saya berpendapat bahawa tekanan dan masalah peribadi mempunyai kecenderungan untuk memberi kesan terhadap pencapaian dan kehidupan seseorang. Masalah kewangan juga boleh menyebabkan individu yang terlibat dengan masalah kewangan akan sentiasa berasa runsing sehingga motivasi kerja menurun. Perkara ini disebabkan seseorang itu sering tiada wang dan akhirnya boleh membawa kepada gejala sosial yang tidak sihat seperti peras ugut, merompak dan lebih serius lagi cenderung untuk membunuh diri.

Kesan moral yang seterusnya dapat dilihat dari sudut daya juang seseorang anggota tentera. Akibat daripada masalah kewangan, semangat untuk melakukan latihan dan operasi akan merosot disebabkan bebanan hutang daripada ceti haram (along) serta badan-badan yang tidak diiktiraf yang tidak mempunyai lesen. Tekanan daripada peminjam disebabkan kadar faedah yang tinggi menyebabkan kebanyakan anggota ATM tidak mampu membayar hutang tersebut dan perasaan takut akan menghantui mereka sehingga tugas serta tanggungjawab terabai. Pada masa yang sama, situasi ini turut mengancam nyawa diri dan keluarga.

Dari sudut kerohanian, tekanan masalah kewangan akan menjadi faktor kepada keruntuhan keimanan yang seterusnya menjurus kepada keruntuhan sosial dan akhlak anggota tentera. Dorongan daripada situasi ini adalah terjebak kepada aktiviti-aktiviti yang tidak sihat seperti pengedaran dan penyalahgunaan najis dadah, merompak, peras ugut dan seumpamanya. Aktiviti-aktiviti ini adalah ditegah dalam konteks perkhidmatan ATM yang merupakan sebuah organisasi keselamatan utama yang diamanahkan oleh Negara dan rakyat secara keseluruhannya. Faktor ini juga secara langsung memberi kesan kepada institusi kekeluargaan yang semestinya akan menyebabkan keruntuhan rumah tangga. Suami isteri akan sering bertengkar kerana sering kesempitan wang untuk menjelaskan sewa rumah, bil-bil, membeli keperluan harian dan sebagainya dan akhirnya sehingga boleh membawa kepada kes penceraian.

Kesan langsung yang wujud akibat daripada pengurusan kewangan yang kurang berhemah adalah dari segi kepimpinan. Masalah yang berlaku akan menyebabkan kurangnya sifat kepimpinan untuk dijadikan contoh atau teladan terhadap anggota bawahan dan seterusnya menjejaskan prestasi organisasi. Disebabkan kepimpinan yang kurang cekap akan menjatuhkan moral anggota bawahan serta penurunan semangat berpasukan dikalangan anggota seksyen, platun atau kompeni. Akibat daripada masalah kewangan juga, kepercayaan dan ketaatan anggota terhadap seseorang ketua akan mudah terjejas. Huraian yang telah dinyatakan diatas jelas menunjukkan bahawa kelemahan dalam pengurusan kewangan dikalangan warga ATM akan menjejaskan moral serta produktiviti anggota tentera. Secara ringkasnya output yang dihasilkan oleh anggota ATM yang bermasalah ini adalah tidak berkualiti dan tidak produktif. Apabila keadaan ini wujud maka berlakulah keadaan yang dikatakan penurunan produktiviti akibat ketidakcekapan anggota ATM dalam melaksanakan tugas dan tanggungjawab ekoran daripada dibelenggu oleh masalah pengurusan kewangan.

Perkara ini perlu ditangani oleh Pegawai atasan kerana produktiviti adalah matlamat utama organisasi. Sekiranya keadaan ini berlanjutan, ianya mampu menyumbang kepada penurunan komitmen serta penumpuan sehingga menyebabkan kurangnya daya juang terhadap objektif utama tentera iaitu menjaga keselamatan negara daripada segala anasir luar. Masalah kewangan dikalangan anggota tentera mampu menjatuhkan motivasi kerja dan seterusnya tidak bersemangat untuk melaksanakan tanggungjawab yang telah diamanahkan.

KESIMPULAN

Rumusan daripada perbincangan ini adalah pengurusan kewangan yang betul dapat membantu mengatasi masalah kewangan yang dihadapi oleh anggota tentera. Sepertimana yang diperbincangkan melalui kesan-kesan yang telah dinyatakan seperti punca berlakunya masalah pengurusan kewangan yang tidak betul, cara-cara mengatasi dan kesan terhadap moral serta produktiviti, jika masalah ini tidak diatasi ianya ibarat duri dalam daging yang boleh menyebabkan pelbagai implikasi buruk kepada individu yang terlibat dengan situasi tersebut. Melalui cara pengurusan yang tepat, secara tidak langsung dapat membantu anggota tentera berjimat-cermat di samping menyimpan wang untuk kegunaan pada masa kecemasan. Semua warga ATM sepatutnya sudah merancang bagaimana membelanjakan wang dengan berfaedah. Jika sikap berhemah diamalkan dalam pengurusan perbelanjaan, kadar anggota ATM berbelanja melebihi pendapatan akan dapat dikurangkan. Justeru itu, dapat ditekankan disini bahawa disiplin sikap yang tegas dan komited terhadap pengurusan kewangan individu merupakan kunci kejayaan kepada kekukuhan kewangan masa hadapan.

BIBLIOGRAFI:

1. Angkatan Tentera Malaysia, 27 Mac 15, http://angkatantentera.blogdrive.com/archive/10.html
2. En. Nasrol Hadi Bin Ahmad Shukeri, 4 Apr 15, http://teknikpengurusanwang.blogspot.com/
3. Norulhuda Sarnon,Jurnal Pembangunan Sosial Jilid 17 Jun 2014,m=59
4. Normah binti Zakaria, 10 Apr 15, http://eprints.uthm.edu.my/4650/4/kompetensi mengurus kerjaya dalam kalangan pesara tentera berpangkat rendah.m=11
5. Berita Harian pada 21 September 2010, 24 Apr 15, http://cuepacs.blogspot.com/2010/09/anggota-tentera-tak-bebas-buat-pinjaman.html

Lt Wilfred bin Semuil telah ditauliahkan ke dalam Kor KPA (Gaji) pada 19 Jan 2013. Beliau berkelulusan Ijazah Sarjana Muda Kewangan dari Universiti Malaysia Sabah dan kini berkhidmat sebagai Pegawai Gaji pasukan di Batalion Kelapan Rejimen Renjer Diraja Para, Kem Terendak Melaka.

INTRODUCTION

The word 'defence' do come with some ambiguity as stated by Whynes; '*...in some countries, it may include the police forces, or the militia*' (Whynes, 1979: 5). For the purpose of this paper, the word 'defence' will refer to a country's standing army, its navy and air force. Additionally, it will also include security forces and the defence administration, where it is financed by the country's expenditure. Malaysia is a democratic country which is constitutionally subservient to or represented by a civil government, and to which a proportion of public funds are devoted towards defence to ensure the integrity and sovereignty of the country. Like many of the countries in Southeast Asia except probably Singapore, Malaysia is considered still as a developing nation where much of its focus is given towards socio-economic development. As stated by Sulaiman that countries in Southeast Asia including Malaysia are more concerned with the development and livelihood of its people where much of the country's income is allotted towards socio-economic development as compared to the needs of defence (Sulaiman. 2009: 91). Sulaiman also states that it is about 'balancing' the apportionment of the country's income between socio-economic development and defence so as to ensure that the sovereignty and integrity of the country remains intact (Sulaiman. 2009: 4).

The distinction between a developed, developing or less developing country can be looked at from differing views. Whynes makes the differentiation through the value of per capita national income or Gross National Product and taking into account all other related factors such as the standard of living, the provision of basic amenities, the level of education or literacy and so forth (Whynes, 1979: 4). However, for the purpose of this paper, developed countries are those countries of the West and countries such as Japan. The less developed countries are those countries such as those in most of Africa. Developing countries are those in between the developed and less developed countries such as Malaysia, Indonesia, Philippines and Thailand. The need for this differentiation is to provide a basis in later discussion of this paper that Malaysia as a developing nation caters more on socio-economic development and to 'balance' its defence budget so as to ensure its integrity and sovereignty remains intact as compared probably a developed country's focus which will ultimately be different and likewise for a less developed country's focus as well.

There is actually no difference between the terms; Gross Domestic Product (GDP) and Gross National Product (GNP). Schiller defined GDP as: '*...refers to the total value of all final goods and services produced in a country during a given time period: it is a*

summary measure of a nation's output' (Schiller, 2005: 32). Truett and Truett defined GNP as: '*...is the market value of all final goods and services produced during some particular time period, such as a year*'. Subsequently, the term 'GDP' will be used as the basis to measure the performance of the Malaysia's economy so as to be consistent with the data collected for analysis in this paper with regard to its defence budget and its defence expenditure.

WORLD ECONOMIC RECESSIONS

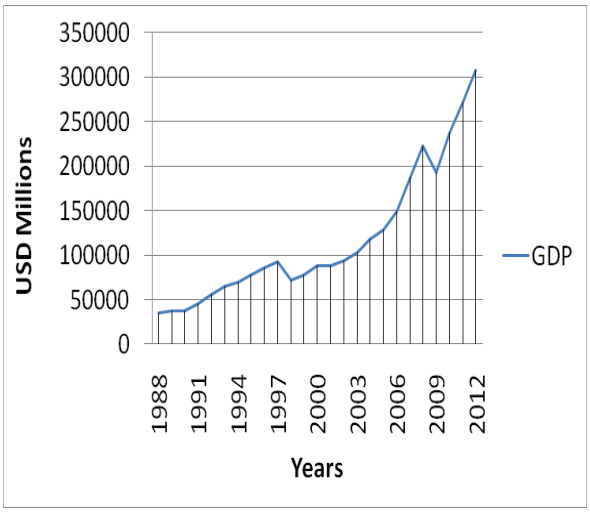
Economic recession is a phenomenon where the national income of a country may be reduced quite dramatically depending on the extent of the impact of the recession to the country. There has been a cyclic of ups and downs of the world economy from the Great Depression of the 1930s to the more recent 2008 recession with the fall of Lehman Brothers and other huge financial institutions that brought down Wall Street and threw the global economy into a major turmoil. More recently, is the debt issue faced by many countries in Europe in 2011 that affected countries of Cyprus, Greece, Ireland, Italy, Portugal and Spain (CNN Library. 2013: 1-7). In the period between the 1930s and 2000s, there were also recessions in the 1940s, 1950s, 1960s, 1970s, 1980s and 1990s (http://www.stocktradingtogo. com. 2008). There were numerous reasons for these instances of recessions such as the impact of Post World War 2 in the 1940s, the Korean War in the 1950s, recession of commodity prices in the 1960s, the Oil and Energy Crisis in the 1970s, the collapse of junk bonds in the 1980s, the financial crisis in the 1990s and the collapse of Dot Com Bubble in the 2000s (http://www.stocktradingtogo.com. 2008). So, when will the next recession be? These trends though not conclusive, reflect that there is a world economic downturn of approximately every 10 years or for every decade there will be some form of economic recession or financial crisis.

In October 2013, the US government had a shutdown due the US Congress deadlocked on the US's debt financing issue but were addressed later but it had shaken markets around the world (The Star Online Business News, 2013). The debt issue does not only involved the US but also involving countries in Europe as stated earlier and is now creeping into the countries in the Far East. There have been reports that China could be facing bad debts that could spark a global recession (Roberts, 2014). China's bad debts, if the analysis is correctly done could trigger serious banking crisis in China that could lead to regional and global economic problems (Roberts, 2014). It is also reported that debt in the Asian region is rising at a worrying pace (Schuman, 2013: 2). Schuman went on to explain that according to Standard & Poor's data; 'lending from financial institutions to the corporate and household sector as a percentage of GDP have risen at a disturbing rate'. The examples Schuman provided were for Hong Kong jumped from 143% in 2005 to 202% in 2012; South Korea from 132% to 166%; Singapore from 91% to 117%, China from 112% to 130% and Vietnam from 66% to 113% in the same time period (Schuman, 2013:2). A more recent report on the debt issue faced by China concerns that it is financing a quarter to a third of its corporate debt to the

tune of USD 14.2 trillion at the end of 2013 through its shadow banking sector (Yap Leng Kuen, 2014: 6) which further confirms the debt issue as reported earlier faced by China. There is a possibility that the next world economic recession could be the result of the debt burden faced by not only the US, countries in Europe but also currently, by countries in the Far East. This recession could come sooner if measures are not adequately taken by governments and financiers around the world. If it does come sooner, there will definitely be repercussions on the Malaysian national income and consequently its defence budget.

In times of a world economic recession, there is a need to provide some means of defence budgeting thatcan address the expected reduction in the budget so as to ensure that the integrity and sovereignty of the country can be safely assured.

MALAYSIAS GROSS DOMESTIC PRODUCT



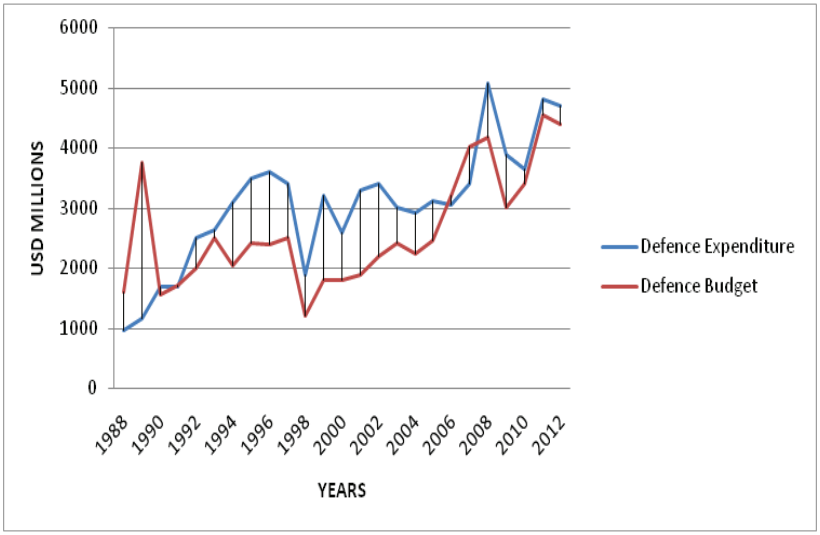
Graph 1: Malaysia's GDP From 1988 - 2012

Data Source: Various issues of IISS's *The Military Balance* 1990-1991 to 2013 and SIPRI's Military Expenditure Database.

Malaysia's Gross Domestic Product (GDP) for the past twenty-five years as shown in Graph 1 above. Malaysia's GDP have more than tripled from USD 72 billion in 1988 to USD 222 billion in 2012. From being an agriculture based country, Malaysia has embraced industrialisation and currently is pursuing to be a fully developed nation by 2020. The successful measures taken by the current and previous governments with the vision of being a developed country by 2020 has been astounding and were recognised by nations the world over. The graph clearly shows that there were a consequent effect on the country's GDP as a result of the Asian Financial Crisis of 1997 and also the melt-down of the world financial institutions in 2008. Besides these two economic 'dips', the country has experienced a continued expansion of its economy as depicted by its GDP

in the Graph below. It also means that Malaysia is not immune to the effects of the world economic recession or financial crisis as Malaysia's trade with its major trading partners involves countries like the US, European Union, China and its closest neighbour, Singapore (Malaysia Statistics Department Report, 2014). China has overtaken Singapore as Malaysia's largest trading partner in terms of exports in 2013 (Malaysia Statistics Department Report, 2014). If any of these countries economy suffers, it will certainly have an effect on the Malaysian economy and thus, its national income.

MALAYSIAS DEFENCE BUDGET AND DEFENCE EXPENDITURE



Graph 2: Malaysia's Defence Budget and Defence Expenditure From 1988 - 2012

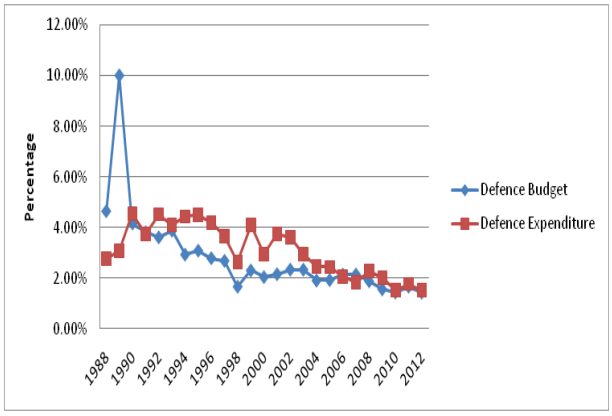
Data Source: Various Issues of IISS's *The Military Balance* 1990-1991 to 2013 and SIPRI's Military Expenditure Database.

From the Graph 2 above, Malaysia's defence budget generally is on the rise for the past twenty-five years. The 'dips' in the graph reflects; the ceasing of the communists arms struggle in 1989, followed by two other 'dips' as a consequent effect of the Asian Financial Crisis of 1997 and the meltdown of the global financial institutions in 2008. Over this time period of twenty-five years Malaysia's defence budget has more than doubled from USD 1.612 billion in 1988 to USD 4.18 billion in 2012. The general trend observed from the graph also reflects that Malaysia's defence budget follows a similar trend of 'dips' in times of economic recession or financial crisis faced by the country. It means that, in times of economic prosperity, the Malaysian government has also increased the defence budgets due to more availability of funds in the government coffers. It also means that the Malaysian Armed Forces has been developed from a counter-insurgency based to mechanisation and to technologically- based organisation. This is evident of the procurement of military assets over these twenty-five years such as Agusta A109s for the Army Air Wing, air-defence systems and tanks for the

Malaysian Army; modern frigates, off-shore patrol vessels and submarines for the Royal Malaysian Navy; F-18 and SU-30MKM for the Royal Malaysian Air Force to name a few (Mahadzir, 2012, 2; Tahyer, 2014, 2 and Apthorp, 2011,1-4). More recently, the procurement of the eight wheeled armoured personnel carriers for the Malaysian Army; the Airbus A400M and the Eurocopter EC725 for the Royal Malaysian Air Force (Mahadzir, 2012, 2; Tahyer, 2014, 2 and Apthorp, 2011,1-4).

However, there were three instances where the Malaysia's defence expenditure experienced a downward movement in the years 1988 to 1990, 1997 to 1999 and in 2008 to 2009. These instances again reflects the ceasing of the communists armed struggle, the Asian Financial Crisis in 1997 and the US meltdown of its financial institutions in 2008 that the respective governments of that period had to take savings measures to cope with the economic situations at that particular point in time. The general trend, however, still points to: in times of economic prosperity, the government of the day were able to spend more so as modernise the Malaysian Armed Forces (MAF) and in times of an economic recession, defence expenditures can be expected to be slashed.

MALAYSIAS DEFENCE BUDGET AND DEFENCE EXPENDITURE AS A PERCENTGE OF GROSS DOMESTIC PRODUCT



Graph 3: Malaysia's Defence Budget and Defence Expenditure As A Percentage of GDP

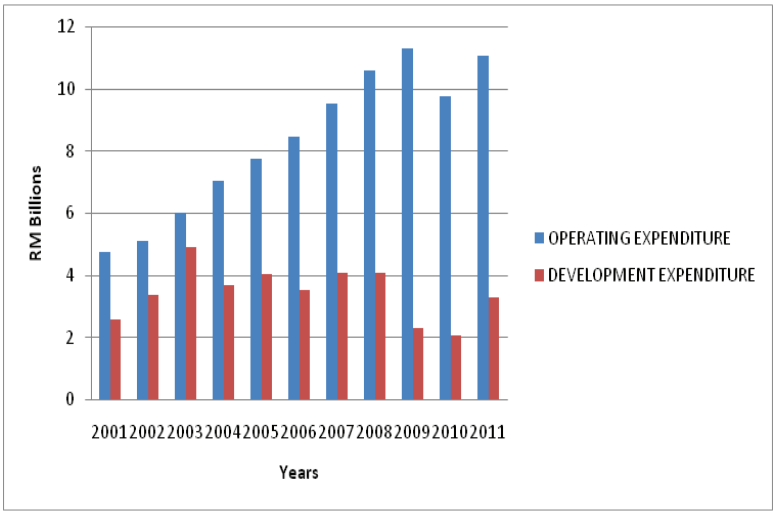
Data Source: Various Issues of IISS's *The Military Balance* 1990-1991 to 2013 and SIPRI's Military Expenditure Database.

Graph 3 above, shows the defence budget and defence expenditure in terms of percentage as compared to the GDP. The general trend reflects that both the defence budget and the defence expenditure are continually on the decline to less than 2% of GDP. That means that it is true to say that the government is focused towards enhancing the livelihood of the people or in other words, to continue giving the priority with the socio-economic development of the country. The apportionment given to defence is like

trying to find a 'balance' to ensure that the sovereignty and integrity of the country is not compromised in the overall nation's budget. Another evolving trend is that the defence budget and its subsequent defence expenditure is becoming almost the same and it may only mean that the government is serious in reducing its debt burden via fiscal measures. However, further research needs to substantiate this new trend with regard to the overall nation's budget over the same period of time.

MALAYSIAS DEFENCE OPERATING AND DEVELOPMENT EXPENDITURES

Graph 4, shows the apportionment between operating and development expenditures with regard to the total defence budget for the time period of eleven years from 2001 to 2011. It can be clearly seen that the general trend since 2001 the portion for operating expenditure (OE) is on the rise as compared to development expenditure (DE). Additionally, if personnel emoluments (PE) has risen and the portion for OE in terms of non-personnel emoluments (NPE) is getting smaller, it can only mean that there will be consequences in sustaining its capabilities level and the readiness of the MAF in times of conflicts and crises. Sulaiman mentioned that a large part of Malaysia's defence expenditure is contributed by the emoluments of its personnel (Sulaiman 2009: 73). A defence analyst findings state that '...intervention in arms procurement without proper consultations with the military has led to problems of interoperability, maintenance and training...' (Singh 2000: 223). If newly acquired military assets are introduced into the MAF and it is not budgeted in the year of its introduction, it may well affect the future capabilities level and the employment of these new assets. If the NPE of the OE is becoming smaller, it may also mean that greater challenges may have to be faced by the MAF in trying to effectively discharged its responsibilities in ensuring the security and defence of the country.



Graph 4: Malaysia's Defence Operating and Development Expenditures 2001-2011

Data Source: Data From the Malaysian Ministry of Defence Annual Reports 2002-2012.

CONCLUSION

In light of the analysis provided here, there is a great likelihood of a world economic depression happening before the end of this decade that may lead to another meltdown in the world's financial institutions due to the debt issue and consequently, the deterioration on the world's economy. It will surely affect the Malaysian economy with rippling effects on the defence budget and may result in smaller allocation for the developmental and operating expenses for the MAF. Thus, Malaysian defence planners need to undertake the necessary precautionary measures to overcome this challenge to ensure that the security of the country can be safely assured during the recession period with possible budget cuts.

From the data analysed above, Malaysia's defence budgets and its consequent defence expenditures over the years since 1988 reflects a general downward trend and achieving a level of not more than 2% of its GDP despite showing an increase in the actual amount for both its defence budgets and defence expenditures. It is very likely that this trend will continue in the future with the fiscal measures taken by the government in its effort the country's debt. The data analysed also confirms that in times of economic recessions or financial crises, there will definitely be a reduction in the defence budget. More importantly, there is a decreasing trend in the apportionment of the defence development expenditure (DE) funds and a marked increase in operating expenditure (OE) funds. A major portion of Malaysia's defence operating expenditures relates to personnel emoluments (PE) due to the increase in its personnel's salaries and allowances.

It is very likely that the trends observed may continue indefinitely until such time the country's debt is more manageable. Pragmatic and practical measures need to be put in place by defence planners and commanders at every level to deal with these challenges so as to ensure that the MAF can continue to safeguard the country's integrity and sovereignty at all times.

There is also a need to rethink of budgetary measures that can assist the MAF in discharging its roles and tasks effectively in times of economic recession or financial crises. There is also a need to incorporate some form of measures in the longer term developmental plan for the MAF for the possibility of economic recession occurrences in every decade.

RECOMMENDATION

There is no best way or perfect solutions to address the budgetary issues of the MAF in times of economic recessions and financial crises as there are a myriad of other factors that have a direct and also indirect influence on the defence budgets and its consequent defence expenditures. However, it is suffice to recommend the following measures subject to further substantiation by other researchers and defence planners

as follows:

a. A minimum budget that is practical and it does not compromise the capabilities level and readiness of the MAF in discharging its duties effectively.

b. The development of human capital in the MAF in areas of economics and finances to ensure a continuity of efforts made by predecessors.

c. The need to relook at the necessary requirements of the portion of NPE in OE that ensures the preparedness of the MAF in ensuring the integrity and sovereignty of the country is not compromised. It means that any rise in PE should also be compensated in a rise in NPE which may not be similar but sufficient enough for the MAF to do its job effectively.

d. Malaysian defence planners need to create some measures in times of budget cuts particularly during economic recessions or financial crises in the longer term developmental plan for the MAF i.e. its strategic development plans. This is to ensure that the development of the MAF can continue unabated so as to guarantee the integrity and sovereignty of the country in the future. Defence can be expensive but it is an insurance that the country could do without in facing the security challenges in the current and forthcoming decades ahead.

BIBLIOGRAPHY

Books

1. Chin Kin Wah (ed). 1987. Defence Spending in Southeast Asia, Issues in Southeast Asian Security. Institute of Southeast Asian Studies. Singapore.
2. Collins, A. 2007. Contemporary Security Studies. Oxford University Press.
3. Creswell, J.W. 1994. Research Design, Qualitative & Quantitative Approaches. SAGE Publication Inc, California.
4. Hartley, K & Sandler, T. (ed). 1990. The Economics of Defence Spending, An International Survey. Routledge. London and New York.
5. Huxley, T. & Willett, S. 1999. Arming East Asia. Adelphi Paper 329. Oxford University Press. Oxford.
6. Mak, J. N. 1993. ASEAN Defence Reorientation 1975 – 1992: The Dynamics of Modernisation and Structural Change. Australian National University. Australia.
7. Malaysian Ministry of Defence Annual Reports from 2002 to 2012.
8. MIDMC, 2007, Readings in Defense Resources Management, Pearson Custom Publishing, Boston, United States of America.
9. Schiller, Bradley R. 2005. Essentials of Economics. Fifth Edition. McGraw-Hill Irwin. New York.

10. Sulaiman, A. 2009. Defence Expenditures of Selected Countries in Southeast Asia. Universiti Kebangsaan Malaysia. Malaysia.
11. The International Institute for Strategic Studies. The Military Balance 1989/1990 to 2012. Oxford University Press. London.
12. Truett, L.J. & Truett, D. B. 1987. Economics. Times Mirror/Mosby College Publishing. St. Louis. Missouri 63146.
13. Whynes, D.K. 1979. The Economics of Third World Military Expenditure. The MacMillan Press Ltd.

Journals/Articles/Monographs

1. Yap Leng Kuen. 2014. Corporate Debt Troubles China. StarBiz. 23 June 2014: 6.

Internet Sources

1. Apthorp, C., 2011. Light Armoured Vehicle Procurement in Asia. Defence Review Asia.http://www.defencereviewasia.com/articles/133/Light-armoured-vehicle-procurement- in-Asia 25/07/14.
2. CNN Library, 2013. European Debt Crisis Fast Facts. http://edition.cnn.com/2013/07/27/world/europe/european-debt-crisis-fast-facts 14/5/2014.
3. Malaysian Statistics Department Online, 2013. Malaysia External Trade Statistics. http://www.gov.my/portal/images/stories/files/Latest_Releases/trade/bi/Jan13/External_Trade_Jan13_BI_pdf 24 Jul 14.
4. The Star Online, 2014. US Congress Enters Crucial Week in Battles Over Budget, Debt Limit. http://www.thestar.com.my/Business/Business-News 14/5/2014.
5. Roberts, D. 2014. China Bad Debt Could Spark Global Growth Slump. http://www.businessweek. com/articles/2014-05-09 14/5/2014.
6. Schuman, M. 2013. Is Asia Heading For A Debt Crisis? http://business.time.com.com/2013/02/25/is-asia-heading-for-a-debt-crisis/ 14/5/2014.
7. ASEAN Defense Policies and Expenditures. Chapter 5. http://www.rand.org/pubs/monograph_reports/ MR1170/MR1170.ch5.pdf, 27/02/2009.
8. Mahadzir, D., 2012, Malaysia Funding Problems Continue, Defence Review Asia. http://www.defencereviewasia.com/articles/152/Malaysia-Funding-problems-continue 25/7/2014.
9. Meinardus, R. 2005. Democracy, the Military and Corruption. Friedrich Nauman Foundation for Liberty Philippines Office. 28 March. http://www.fnf.org.ph/liberalopinion/democracy-military-corruption.htm 05/11/2009.
10. Reinkensmeyer, B., 2008). Timeline of 17 Recessions and World Crises Since Great Depression. http://www.stocktradingtogo.com/2008/07/18/timeline-of-all-recessions-and-world-crises-since-great- depression/ 25/07/14.

11. Stockholm International Peace Research Institute (SIPRI) Military Expenditure Databases http://milexdata.sipri.org/24/07/14.
12. Tahyer, C., 2014, 1-6. Southeast Asian States Deploy Conventional Submarines, The Diplomat.
http://thediplomat.com/2014/01/southeast-asian-states-deploy-conventional-submarines/ 25/07/14

Kol Amirudin bin Dato' Sulaiman was commissioned in 1985. He holds a double Master's Degree in Defence Studies from University of Canberra and UKM. His current appointment is as the Director of Strategic Management, Malaysian Armed Forces Headquarters with the Defence Plans Department. He has held many important appointments such as SO 1 Strategy/Concept at the Planning and Development Branch at the Army Headquarters, Commanding Officer of the 1st Battalion Border Regiment, Colonel Doctrine at the Army Training Headquarters. Prior to his current appointment, he was the Chief of Staff at the Army Training Headquarters.

THE IMPLEMENTATION OF CYBER SECURITY AWARENESS IN MALAYSIAN ARMY TRAINING CENTRE

by Mej Syed Kamalluddin bin Syed Mokhtarruddin

In the last one decade demonstrated the immense application of Information and Communication Technology (Information and Communication Technology) or ICT among government employees. ICT has been used to change the way services are presented. Simultaneously, it creates a positive change in the working culture, reduce operating costs and increase productivity as well as quality of service. ICT also used as a mean of communication for information delivery between personnel and organization management.

As an organization which concerned with the speed and accuracy of decision-making, Malaysian Army (MA) is no exception. These days most of the officers and members of MA work in an environment that uses ICT. They manage and control information using a variety of ICT devices either their own or belong to their office. At the same time, they use Internet as a medium of communication in cyberspace. They communicate using a variety of applications that are available through the websites, especially social media networks such as Facebook, Twitter, blogs and news portals. However, they did not realize that they expose themselves to the threat of information leakage. It is like pouring salt into the wound, the threat is exacerbated due to evasive attitude of management and the absence of control mechanisms of information security at the higher level.

In today's rapid advances in ICT has changed the approach in every aspect of life. In the military context, the prospect of ICT combined with sound doctrine and organization will allow the armed forces to disable his opponent with big impact. This capability described in the theory RMA (revolution in military affairs) which it refers to how the revolution in defence technology has changed the approach of war that will happen in the future. Successful countries which adapt the advantages of this revolution will certainly get a force multiplier to their armed forces. These advantages are referred as the advantages of information (information superiority) compared tothe adversaries.

Before we go to very detailed on cyber, we need to understand whatis cyber is all about? From dictionary.com, cyber mean [1]a combining from meaning “computer”, “computer network” or “virtual reality”, used in the formation of compound words (cyber talks; cyber art; cyberspace) and by extension meaning “expressing vision of the future”.

1. http://www.dictionary.com/browse/cyber-

From oxford dictionary[2], cyber is relating to or characteristic of the culture of computers, information technology, and virtual reality. This mean, cyber is always related to computer, virtual and network. It also means cyber is not simply we can use our hand to get it. It is controlled by technology. Nobody can stop it.

While, generally security means protecting assets owned. It means protecting assets from the threat of hackers, natural disasters, power failures, theft and various undesirable situation. While information security is defined as a situation in which all things design and supply services based on ICT systems run continuously without interruptions that could affect safety. Information is said to be safe when three key elements are met, namely confidentiality, integrity and availability.

Definition from Wikipedia[3], cyber security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. The field is of growing importance due to the increasing reliance on computer systems in most societies. Computer systems now include a very wide variety of "smart" devices, including smart phones, televisions and tiny devices as part of the Internet of Things–and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks.

In our culture today, there are many misused of this technology. As an example there are cyber bullying, hackers, virus attack, viral and much more. It is very easy for us to get information today. Just use a finger and put it on the screen and touch button search. There are a result of our search will appear then. People feelenthusiastic on cyber to get information daily. If their internet not function a day, they will shouted to the service provider to get it.

Some people argue that information security threats in cyber space are just theories. While others believe it is a very serious matter and can be considered a threat to national security. However, it is the fact that many information security incidents reported worldwide following the hacker activity or due to negligence of the user as well as the weakness in the organization itself.

The incidents of information security have been widely reported around the world prove that the threat is becoming increasingly serious proportional to the use of ICT. However, according to a study by James Cloburn in 2008 found that only 11 percent of organizations involved in security breaches report the incident. This proves that the

2. http://www.oxforddictionaries.com/definition/english/cyber

3. https://en.wikipedia.org/wiki/Computer_security

information security threats are more serious than those reported by the mass media. This fact should be taken as a lesson by all agencies to strengthen their own organization's information security defence.

Today, our military personnel need to educate for them to understand how to implement cyber security in their live? Therefore, the education needs to come from our school as an early education when they started to join army. For other rank, there are a PUSASDA and for officer there are ATD - Officer College and National Defence University that will provide them this education. Our service just got a PUSTEKMA, Cyber Warfare Department in BSPP, Computer Cell in KOMLEK and much more. But this still not enough for us to counterpart what will happen when people just ignore about cyber security? The important thing is how to implement cyber security in Army School?

First of all we need to know what the vulnerability that related to cyber. From Wikipedia[4], vulnerability is a system susceptibility or flaw, and much vulnerability is documented in the common vulnerabilities and exposures (CVE) database. Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. The threats or vulnerabilityidentified as backdoors, denial-of-service attack, direct-access attacks, eavesdropping, spoofing, tampering, privilege escalation, phishing, click jacking and social engineering and Trojan horses.

In the aspect of information security, technology alone is not enough for an organization to survive cyber attacks. In addition to technology and processes that provide basic security to the organization, the human factor should be given serious consideration. Information security experts have recognized the need to educate and manage the human aspect in the field of information security. As users, they should have necessary knowledge and skills in regard to information security.

Therefore, all users who handle the classified information should be given basic knowledge when operating in cyberspace. In the context of the MA, they must fully understand the classification of information as stipulated in Government Security Directive and Malaysian Armed Forces Security Instruction (FSI). Control must be optimized by using encryption technology, digital signatures or any other mechanism that can protect information.

In order to assist the understanding of users, basic training should be implemented by each organization on a regular basis. Such training should cover all users from various levels in the organization. In addition, information security training cooperation can be made with various external parties such as the Cyber security Malaysia, MyCERT, consultants and other cyber security agencies. Through this exercise people will be exposed to a special ethics when interacting in cyberspace such as forums, social

4. https://en.wikipedia.org/wiki/Computer_security

media networks and blogs. Ethics will help so they do not fall into a situation that could give legal implications afterward.

In addition to enhance the understanding, the other important aspect is the awareness to end-users. Users should be trained in order to have the awareness of information security at all times. Awareness means having or discloses conscious perception or knowledge means alert when watching or ready during the conclusion compared with something that has been experienced before. In this case, users who have an adequate level of training should have a high level of cyber security awareness.

Generally, awareness can be divided into user awareness and management awareness. User awareness allows users to prepare themselves toward threats to their information environment. Whereas management awareness plays an important role because they will determine the direction of policy and program in their organization.

End-users awareness can be established by means of training, courses and so on. Awareness training to users should begin with awareness training. Security awareness training is a preventive measure that will help users to understand the benefits of good security practices. This awareness training can be developed through programs such as the internal organization of lectures, exhibitions, posters and stickers. These programs should focussing users to change behaviour and attitudes as well as motivate them to protect the information assets of the organization. The programs should be designed not only be apply to all users, but also need to fulfil the basic cyber security requirements of different groups within the organization.

In the context of management awareness, the organization must have a specific mechanism to control and prevent threats to the security of their information. Furthermore, top management should have a special insight to ensure that their organizations have a certified safety standardwhich recognized at the international level. Unfortunately, most organizations which make procurement information system are only concerned with the acquisition of physical assets and less concerned about the importance of the documents governing the use of those assets. The importance of these documents only revealed after security incidents occur that normally relates to the weaknesses in terms of control and enforcement of policies or procedures.

In addition to the awareness of information security, users need to be exposed to the advanced knowledge and skills in information security. They should be well familiarized with the operating system and network environment they are using. These skills can be achieved through a special allocation by attending appropriate training courses. In addition, an internal training concept can be implemented in order to train the trainer courses which training costs can be saved, thus making those who attended the course more focused and accountable. However, users should not be too dependent on the organization for information security knowledge. There are many online resources and books related that can be referred in order to enhance cyber security knowledge.

As far as the security experts are concerned, cyber security threat is an internal threat to our military service. We don't need to wait for other country to attack us. We ourselves attack our information and transfer it to our enemy. Our enemy only needs to browse from the Internet to get information about our armament, our organization chart, our secret plan, our human resource plan, our logistic plan and much more. We need to bring these issues to our top branch and discuss it seriously. We need to stop this habit.This habit become a virus and can paralyze our defence system. As I mention earlier, we are attacking by our own people and our own man. They don't understand what the implication to our nation when they practicing this habit. How to know all the Vulnerability? Even though wedid not have dedicated and specific education on this matter. Some rather how our personnel were came from difference type of education. Only a few have dedicated education like First Degree and Bachelor Degree on this matter. That's why we need to give an education and enforcement to make sure all our data is saved.

Educations start from school. Our army school need to fulfil with dedicated education and information. We need to form up a new organization on our Training and Doctrine Headquarters (TRADOC HQ) a special team that come with designated post that only task for the cyber security. This post need to put behind training management organization. They need to build a training management planning (RPL) on this subject. They need to organize, educate and give some lecture to our personnel especially new generation. They also been task to monitor our personnel activities especially on social media and bring feedback to our top branch if they find abnormal activities. We must give them a special task that not jeopardizes other staffing work in the HQ.

Our dedicated school also need to be a specialized on this matter. We need to promote our school as a cyber-entrepreneur that expert in cyber security. All our school can organize small seminar that will invited other army organization such as Division and Bridgedlevel to attend. Our school need to get support from our dedicated organization such as MK TD - PUSTEKMA and MATM - KOMLEK. Our school must be the founder of cyber security education. In order to contribute for this matter, we need give and get a proper outsider course that related to this subject. This will bring our school to lead on subject cyber security.

We also need to collaboration with other agencies. There are a lot of agencies that will help us to gain knowledge and get information on important of cyber security. Our government had developed several agencies under Ministry of Science, Technology and Innovation (MOSTI) in order to make sure our country save from cyber-attack and other enemy. The well-known agencies were Cyber Security Malaysia[5]. Their vision is to be a globally recognised National Cyber Security Reference and Specialist Centre by 2020. Their mission is to create and sustain a safer cyberspace to promote National Sustainability, Social Well-Being and Wealth Creation. Their core values were Trust,

5. http://www.cybersecurity.my/en/about_us/vission_mission/main/detail/2064/index.html

Impartiality and Proactive. Trust means by maintaining social, ethical and organisational norms, we firmly adhere to codes of acceptable conduct and professional ethical principles. Impartiality mean by providing consultation, advice and decision making with professionalism based on established facts and rationale, and devoid of any personal or conflict of interest and bias. Proactive mean by taking prompt action to accomplish objectives; anticipating challenges and identifying early solutions; taking action to achieve goals beyond what is required or expected.

We need to collaborate with these agencies in serous manner. There also a government sector that eager to give their service and expertise in professional manner without gain any profit from us. We need to get their support. The important thing we must know what service they can provide. They are provided service MyCERT - The Malaysian Computer Emergency Response Team. This team (MyCERT) consists of Specialists and Analysts in the areas of Incident Handling and Malware Research. They also provided Digital Forensics, Data Recovery, Data Sanitisation and Expert Witness. Much more facilities that we can get from them.

We also need to give an attention on Celebration of Safer Internet Day (SID)[6]. It was first held in year 2004 initiated by INSAFE EU. These celebrations were celebrated in over 100 countries globally in February of each year to promote a safer Internet, nurturing and increasing public awareness on cyber security. This year is the 13th celebration that was happen on 9th February 2016.The theme for the day was 'Play your part for a better internet', encouraging all stakeholders – children and young people, parents and carers, teachers and educators, and industry and politicians – to celebrate the day and play a personal role in helping to create a better internet for all, but especially for children and young people. They are also urged to play their roles more ethical and more responsible when using Internet. To encourage our personnel to have some awareness about cyber security, we need to join this celebration and make some interesting activities like organize an exhibition, seminar, classes and much more. Full support from high formation is much needed. When the awareness is around us, this automatically will give us some opportunity to enhance the information to family and friend. By having the understanding and knowledge about Internet Safety, we can make full use of knowledge by creating a secure and conducive cyber environment.

To be a good Internet leader, we need to take these 3 important words. It is Thinker, Inspirer and Proactive[7]. The thinker word means we need to identifying online Frauds and taking necessary prevention. This action need to take by us by providing our ICT facilities with antivirus and firewalls. Inspirer means we need to build a positive online reputation by practicing good Internet ethics. As an example we need to practice ourselves for never post inappropriate or embarrassing material anywhere on the

6. https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694959

7. https://www.betterinternetforkids.eu/

Internet. The last one is proactive. As an Internet user we need to proactive by engaging in sustaining a better Internet for all. We need to practice by setting a private account on personal computing, changing password every 3 month and much more ethic for using Internet safely.

Personnel interest in reading need to increase in order to gain information. They need to read a book, article, browsing internet and many more to get information about security in cyber space. There are no limitations or border for us to cross in order to find some information. As we know our reading icon was Tun Dr Mahathir Mohamad. This we can read from http://ww1.utusan.com.my/utusan/Rencana/20120514/ re_01/Dr.-M-ikon-budaya. Our country also very concern on reading behaviour. We need to increase and give some recommendation to our personnel on reading matter. The reading skill will develop when we make it as a habit. One day one book to read. Many of us always give some reason and did not want to read severally. Other benefit we can get from reading are we can talk on something difference from others that did not like to read. We also not shock when we heard something new because it is continuity from our last reading. This process need to be continuity to entire life.

Cyber world are very huge world. There is non-stop activities happen there. As an army, we need to get some information and distribute it between organization and personnel. The knowledge need to enhance every day. We need to take all opportunity giving and service provided by our services, government and management to face this reality. We need to get supportive from all around us that have a good facility, good courage and more informative training. Therefore, Malaysian Army Need to Give More Attention to this issue. Our organization need to give more attention about this matter.

Commitment from our organization towards the use of ICT for defence development will increase the dependence on cyberspace. Cyberspace is borderless world that has its own identity. According to Internet World Statistic, until June 2010, Internet users are estimated at 1.97 billion. If we assume the cyber world is a country, then it will become a country with a large population of the world. One of the main challenges in the cyber world is abuse, hacking and the most feared is cyber war. The information revolution is the Internet misused for illegal activities such as spreading false information, e - mail espionage, credit card fraud, spam and so on.

Cyber criminals are moving borderless. Cyber criminals can act without arms or sophisticated or expensive military capabilities. Someone cyber criminals may be able to transfer money to RM5 million from a bank in Kuala Lumpur to a bank in Tokyo in just a few seconds. Criminals do not need warships or missiles to disable CNII[8] operation. Whether the information is true, partially true or not true will be spread and shared by the people of the cyber world. Because of this, many countries in the world makes cyber agenda as a national agenda. Our Malaysian Army also need to take cyber as a serious

8. CNII - About Critical National Information Infrastructure

issue and discussion among personnel. We need to transform to be more sophisticated and reliable to our country as a main defence to national security.

Army Training and Doctrine Headquarters as Army School management need to foresight and be ready with such information. This institution need to give a first priority in Army organization to get best facilities on cyber matter. We need to give attention on man, method and machine in order to make sure all cyber thread and internal thread become our friend and not our enemy.

In conclusion, incidents that occur throughout the world represents a new dimension of information security threats. The fact that should be accepted by all parties especially when the consequences of the cyber security breaches can cause a serious impact on all organizations. Thus, prevention is the most effective measure to prevent these devastating consequences from happening.

Factors that play a significant role in protecting the security of information such as policies, procedures, management and human should be given a special focus. All users, administrators, managers and senior officers must have initiative, not least to prepare themselves and their organizations to face the threat of information security challenges. For a start, all parties need to broaden the horizon of thought to strengthen the security aspect of information and thus take proper steps to achieve this. Hopefully one day, we will all be able to optimize the use of ICT in order to make our country to become an industrialized nation which excelled in various fields.

BIBLIOGRAPHY

1. Definition of Cyber security - http://www.dictionary.com/browse/cyber-
2. Definition of Cyber security - http://www.oxforddictionaries.com/definition/english/cyber
3. Definition of Cyber security https://en.wikipedia.org/wiki/Computer_security
4. Related of Vulnerability - https://en.wikipedia.org/wiki/Computer_security
5. Organization CyberSecurityMalaysia - http://www.cybersecurity.my/en/about_us/vission_ mission/main/detail/2064/index.html
6. Safer Internet Day (SID) - https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694959
7. Good Internet Leader - https://www.betterinternetforkids.eu/
8. https://www.facebook.com/CyberSecurityMalaysia/?fref=nf

Mej Syed Kamalluddin bin Syed Mokhtarruddin (3008526) telah menyertai Tentera Darat Malaysia semenjak Tahun 2000 dan sekarang sedang berkhidmat di Markas Latihan Tentera Darat, Kem Segenting, Port Dickson, Negeri Sembilan sebagai Pegawai Staf 2 Pengurusan Sistem (CPS). Pernah berkhidmat di beberapa pasukan seperti 4 Skn RSD Mek sebagai Ketua Terup Radio dan 74 SSD GAPU sebagai Penolong Ketua Skuadron. Di Markas Formasi pula pernah menjawat jawatan Pegawai Staf 3 ICT di Markas Pemerintahan Medan Tentera Darat dan Ketua Detasmen P4 di Markas Briged Keenam Infantri Malaysia. Dari segi pendidikan pula, beliau mendapat pendidikan awal di Sekolah Rendah Al-Islah. Kemudian mendapat pendidikan menengah di Sekolah Menengah Islam Hira'. Seterusnya melanjutkan pelajaran di Akademi Tentera Malaysia dan telah dianugerahkan Ijazah Sarjana Muda Kejuruteraan Komputer (UTM-ATMA) pada tahun 2005.