KnE Social Sciences

ICoSaPS Conference Proceedings
The 3rd International Conference on Social and Political Science
"The Impact of Information Technology on Social and Political Dynamics", (2016), Volume 2017

Knowledge E
Engaging minds

Conference Paper

The Off-line and On-line Impact of Information and Communications Technology on ASEAN Security — a Perspective

Bilveer Singh

Department of Political Science, National University of Singapore
Centre of Excellence for National Security, RSIS, Nanyang Technological University, Singapore

1. Introduction

Modern information and communication technologies have brought immense changes to peoples' lives in the developed and developing countries. It has been a revolutionising game changer impacting on the manner people communicate, do business, partake in crime and even harm others physically and psychologically. This is increasing as the rate of technologies, especially the Internet, penetrate deeper into populous countries in Asia and Africa. Its role has been so immense and pervasive that it has led to all-round changes in the manner societies organise themselves, including in the security arena. The benefits of these technologies have been massive, changing exponentially the manner governments and people connect with each other within and without the territorial state.

However, if these technologies can benefit communities at large, they can also be harnessed by elements intending to cause harm, be it criminals that are intent on theft or terrorists that have been able to leverage on these technologies to achieve their goals, be it in terms of undertaking radicalisation or even coordinating attacks. The uploading of manuals on how to launch attacks, kill people and even to make bombs, have also been exploited through these new mediums of information and communication technologies. It is due to this factor that some have argued that after land, sea, air and space, cyber space has emerged as the fifth domain of warfare.

2. Understanding the Information and Communication Technology 'Beast'

First, what is Information and Communication Technology or ICT? As a generic term it is used to describe the various communication applications and devices, including among

Corresponding Author:
Bilveer Singh

Received: 09 April 2017
Accepted: 17 May 2017
Published: 12 June 2017

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICoSaPS Conference Committee.

others, radio, television, cellular phones, computer hardware and software, and satellite systems. According to Ifueko Omoigui Okauru, it involves digital processing that involves the storage, retrieval, conversion and transmission of information [1]. Often, it is synonymously used to refer to computers and computer networks. Increasingly, this has come to encompass personal computers, laptops, tablets, mobile phones, transport systems, televisions, and network technologies. The one area where ICT has made a massive impact is the Social Media. In addition to the Internet, this can encompass the YouTube, Facebook, Twitter, chat rooms, discussion forums and now, the difficult to track and penetrate, the Telegram.

The penultimate area, which has come to affect Mankind is the use of ICT in cyber space. As every nation, have become interconnected within and without through technology, this has also exposed them to all kinds of attacks and hackings. Due to technological accessibility, there are two major distinct groups of hackers, state and non-state. Non-state actors include common criminals, terrorists and 'hacktivists' who engage in the non-violent and even violent use of illegal or legally ambiguous digital tools in pursuit of political ends. Some hacktivists have used their technical knowledge for vandalism or protest. Notorious groups such as Anonymous have stolen and leaked classified information from government, banks, or other high-ranking establishments and institutions. The second source of cyber threats emanate from state-centric actors. These state actors are keen to obtain insights into other countries' political, strategic plans, research and development as well as manufacturing and technological know-how, or to hack into essential national infrastructure systems, possibly for military exploitations.

With the rise and importance of information technology in almost every facet of public and private lives, and the willingness of state and non-state actors to gain information both legally and illegally, this new frontier has become highly competitive, something that is benefitting Mankind and yet, has the potential to cause much harm. Hence, there is a duality in understanding the concept of security: in the positive sense of promoting a better quality of life and in the negative sense of preventing being harmed.

3. How can ICT affect National Security?

ICT is amoral. It can facilitate security or be used by people to enhance insecurity and threats. While governments have harnessed ICT to enhance national security through networks at border controls to detect illegal crossings through fake passports, etc. at the same time, ICT has been a major game changer for terrorists to facilitate their modus operandi. While modern information technology is a boon for multiple activities, it can also be a bane. This was most clearly evident in various cyber-attacks that

have taken place in the last few years. This can involve hacking into banking accounts, government departments, credit card companies, entertainment companies (Sony and PlayStation), medical records, internet accounts (Yahoo), and corporate espionage. So far, in 2016, the following cyber-attacks have taken place: *Janesville computer systems hit by virus, likely 'ransomware'; Virus hits city server; resident data not likely breached; Cryptocurrency-Backed Venture Capital Fund Hacked; Ether Plunges; Russian government hackers penetrated DNC, stole opposition research on Trump; North Korea hacked 140,000 South Korean computers in a huge campaign; Dell Official Website Subdomains Hacked By Kurdish Hackers; Karnataka Police website hacked; Scrum.org hacked, may have lost crypto keys and some user data; Overwatch servers down in possible Lizard Squad DDOS attack; and Muslim Brotherhood's Website Suffers DDoS Attacks and Data Leak*.

The other key cyber-attacks include the following:

1988

The Morris worm -one of the first recognised worms to affect the world's nascent cyber infrastructure- spread around computers largely in the US.

DECEMBER 2006

NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked.

APRIL 2007

Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Government and commercial institutions were targeted.

JUNE 2007

The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.

OCTOBER 2007

China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas.

SUMMER 2008

The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

AUGUST 2008

Computer networks in Georgia were hacked by unknown foreign intruders around the time that the country was in conflict with Russia.

JANUARY 2009

Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers.

JANUARY 2010

A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu.

OCTOBER 2010

Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear programme.

JANUARY 2011

The Canadian government reported a major cyber-attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence.

JULY 2011

In a speech unveiling the Department of Defense's cyber strategy, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.

OCTOBER 2012

The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007.

MARCH 2013

South Korean financial institutions as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.

MARCH 2014

In May, eBay revealed that hackers had managed to steal personal records of 233 million users. The hack took place between February and March, with usernames, passwords, phone numbers and physical addresses compromised.

OCTOBER 2015

The White House's unclassified network was hacked, accessing the president's schedule and emails that revealed personnel moves and policy debates.

Hence, the double-edged character of ICT. While it has brought widespread socio-economic benefits to even the most remote corners of the world, it has also empowered those who seek to destroy and disrupt.

4. ICT and Terrorism

While the use of information technology for malicious purposes, especially for political goals or financial benefits has been clearly documented, what is increasingly disconcerting is the application of information technology for terrorism and the spread of extremism. A RAND study was particularly instructive in this regard with regard to radicalisation. In the literature with regard to the Internet and radicalisation, the report identified the following five hypotheses:

1. The Internet creates more opportunities to become radicalised.
2. The Internet acts as an 'echo chamber', a place where individuals find their ideas supported and echoed by other like-minded individuals.
3. The Internet accelerates the process of radicalisation.
4. The Internet allows radicalisation to occur without physical contact.
5. The Internet increases opportunities for self-radicalisation.

The above hypotheses would tend to describe the Internet, in this case, the high-end symbol of modern ICT, as the key enabler of radicalisation. Why is the Internet, through the use of ICT and its operations in cyber space, increasingly a weapon of choice for the terrorists? This stems mainly from the various advantages and benefits such a technology allows as far as attaining the goals and objectives of the terrorists are concerned. The terrorists have resorted to ICT and especially the Internet due to the following reasons.

First, it is easy to access. Second, it is due to the decentralised structure with little or no regulation or governmental control provides advantages over other platforms such as off line publications. Third, it has immense potentiality for a worldwide audience and with great immediacy, especially since it is not limited to any geographical boundaries. Fourth, it provides anonymity of communications which perpetrators of terrorism would prefer. Fifth, there is the fast flow of information. Sixth, it is generally inexpensive and easy to maintain, especially the web presence. Seventh, with rising multimedia environments, this platform is easily used and accessed with great efficacy. Finally, it is also able to shape coverage in the traditional mass media.

In view of the obvious reasons for using ICT, what do terrorists use cyber space for? The terrorists use cyber space and the accompanying ICT for the following purposes:

1. Data mining
2. Information and online presence
3. Online communications
4. Dissemination of propaganda and publicity
5. Networking
6. Movement of personnel to combat zones or to targets identified for attacks
7. Planning and preparations
8. Recruitment
9. Training [real or virtual]

10. Financing
11. Indoctrination and Radicalisation
12. Purchase of arms and explosives
13. Organising attacks
14. Cyber theft and fraud
15. Cyber attacks

Due to ease of access, affordability and effectiveness, ICT has helped to enhance national threats as it has acted as a force multiplier for those who intent on harming society. Hence, while ICT has brought immense benefits for communications, information gathering and sharing, and even businesses, it is a double-edge sword that has the capability to enhance all-round insecurities. Today, an individual need not travel overseas to be radicalised as self-radicalisation is a possible avenue through the Internet and Social Media that is facilitated by radical-oriented websites through ICT.

5. ICT and Security Threats in Indonesia

ICT-related threats are not new to Indonesia, as they are elsewhere. However, what is disconcerting is that Indonesia, according to a 2013 survey by Akamai Technologies, an IT security firm, "had overtaken China as the number one source of hacking traffic in the world" [2]. Muliaman Hadad, the Chairman of the Financial Services Authority (OJK), cited 36.6 million cyber-attacks in Indonesia in the past three years since 2013 [2]. This substantial increase, almost double its first-quarter traffic from 21% to 38% of the overall global total, pushed China into second place even though with a still substantial 33%. Between these two nations they accounted for almost three quarters of all cybercrimes in the world [3]. With the increasing popularity of e-commerce in Indonesia, it also meant that there were more online transactions, providing greater opportunities for hackers to exploit security loopholes. Since 2010, most of the attacks in Indonesia were attributed to China, South Korea, the USA and Russia.

The perpetrators of these crimes are not just Indonesians but also foreigners. In April 2016, it was reported that 31 Taiwanese were arrested in Indonesia for cybercrime offences, referred to as telecom fraud. Operating from Balikpapan City in Kalimantan, the Taiwanese were suspected of using Indonesia as a base for cybercrime against Taiwanese and Chinese citizens [2]. In August 2015, through joint operations of Chinese, Taiwanese and Indonesian police, Indonesian law enforcement officers dismantled an international fraud ring based in Indonesia, arresting 82 Taiwanese suspects and seized

US$762,994 in cash [4]. As Indonesia, the largest market in ASEAN, is a key node in the global trade and in the context of rising economic cooperation, there is the growing concern that critical banking and other data may be breached through hacking, thereby undermining trading through the Internet and *e-commerce.*

However, while cyber criminals are globally widespread, of late, it has been the role of ICT, especially the Internet and Social Media in facilitating terrorism and terrorism-related crimes in Indonesia that has gained much attention as far as what ICT means for the security of nation states. Sufficient research exists to confirm that ICT, especially through the Internet, Social Media and new technology platforms such as the Telegram, have been used to facilitate, among others, the following acts relating to terrorism and extremism:

1. Open and encrypted communications among terrorist networks in Indonesia and with transnational terrorist groups abroad.
2. Radicalisation through access to radical websites, front line videos and preaching by radical ideologues.
3. Recruitment of sympathisers, supporters and fighters.
4. Links and cooperation among terrorist networks at home and abroad.
5. Collection of funds often referred to as 'terrorist financing' through donations or transfers from other terrorist groups.
6. Cyber terrorism including hacking into government websites and defacing contents of government websites.
7. Training
8. Launching operations including learning how to make bombs.
9. Cybercrimes in the name of *Fa'i* [legitimate loot of an enemy in war].

Already, there are more than 250 radical websites propagating messages and support for the Islamic States. These are mostly in Bahasa Indonesia. Additionally, Arabic radical videos are uploaded on various Social Media sites, including U Tube and Telegram with Indonesian subtitles.

An example of information technology being used for terrorism-related crime in Indonesia was elucidated by Brata Adisurya:

> *Densus 88 Antiteror Mabes Polri telah menangkap salah seorang yang diperbantukan pada Tim Pembela Muslim (TPM) selama persidangan di Semarang. Orang tersebut adalah Agung Setyadi (35), seorang dosen Fakultas Teknik Informatika Universitas Stikubank (Unisbank) Semarang. Agung ditangkap*

anggota Densus 88 Mabes Polri, di rumahnya, Jl Sriwijaya Semarang, sekitar pukul 12.00. berdasarkan keterangan yang dihimpun di Jakarta, Mabes Polri telah menangkap pembuat website beralamat www.anshar.net yang dipakai untuk menyampaikan informasi terorisme. Dua pembuat situs ini ditangkap di Semarang. Dua tersangka yang ditangkap itu adalah Mohammad Agung Prabowo alias Max Fiderman alias Kalingga alias Maxhaser dan Agung Setyadi. Menurutnya, Max adalah mahasiswa Fakultas Elektronika sebuah universitas di Semarang. Max ini memiliki kemampuan di bidang teknologi informasi, khususnya hacking dan carding. Isi laman atau website www.anshar.net, sesuai dengan pelacakan yang dilakukan Densus 88 Antiteror, adalah informasi soal penyerangan dengan cara memanfaatkan antrean masuk jalan tol, kemacetan lalu lintas, pintu keluar-masuk kantor, mal, pusat hiburan, pusat olahraga, hotel, dan tempat pameran. Dalam laman itu juga termuat target yang diincar jaringan terorisme di Indonesia. Antara lain Ancol, Planet Hollywood, Senayan Golf Driving Range, dan Jakarta Convention Center (JCC). Halaman tersebut dibuat pada Juni hingga Agustus 2005 atas permintaan Qital alias Abdul Azis (tersangka dalam kasus bom Bali II). Qital membuat laman itu atas perintah Noordin M Top yang kini masih buron. Untuk membuat laman, Qital sebelumnya telah meminta bantuan Agung Setyadi. Agung lalu meminta batuan kepada Max untuk membuat laman karena Max memiliki keahlian di bidang teknologi informasi. Lewat percakapan di internet itulah, sesuai dengan pengakuan Agung Setyadi, Qital bisa berhubungan dengan Max hingga akhirnya terbuatlah situs www.anshar.net. Untuk membuat program itu, Agung dan Max membeli satu laptop dengan membobol kartu kredit milik orang lain (carding). Dari kasus tersebut, lanjut dia, terungkap pula, mereka juga menggalang dana untuk kegiatan terorisme dengan kejahatan yang memanfaatkan teknologi informasi [5].

There have also been other more ambitious information technology-related terrorism acts in Indonesia. Ansyaad Mbai, the former Head, Counter-Terrorism Agency of Indonesia (BNPT) revealed in his book that between August and November 2011, Indonesian terrorists linked to Mujahidin Indonesia Timur led by Santoso, with cyber skills, namely, Rizki and Cahya, "managed to hack into the online investment site 'Speedline' [belonging to a Multi-Level Marketing firm]. Through this cybercrime, they managed to steal more than 7 billion Rupiah. The stolen loot was to be used to finance jihadi operations in Poso, such as the purchase of weapons, military training and other related activities. This idea was approved by Santoso. One of the main programs to be implemented on an urgent basis was military training" [5].

6. What to do and Challenges Ahead

Clearly, while information technologies have been helpful, this is not the full story. While there are benign uses, it can also be unleashed by maligned forces. To overcome threats while sustaining its positive knock-on effects, there would be the need for robust national measures as well as regional and international cooperation to tackle cybercrimes and attacks. The aim would be to pre-empt, deter and neutralize cyber-attacks and the use of such technologies for harm purposes. This would entail the hardening of hardware and software that are involved in information technologies provision and their related platforms. In this regard, many countries have resorted to establishing a National Cyber Agency to counter cyber-related crimes. Some sovereign systems have also mobilized and activated 'çyber-warriors' to counter online radical narrative and messages of the jihadists and their supporters.

Yet, at the same time, as the terrorists and their co-workers realize that their use of the cyber space is being targeted and increasingly penetrated, they have shifted towards the encrypted apps or domains such as *WhatsApp,* Telegram and even the Darknet. This is beginning to pose serious challenges for the law enforcement agencies as it is becoming difficult to access these domains and track them. At the same time, there is also the jurisdictional and privacy issue that is constraining law enforcement. How does one retrieves information legally in different legal domains and where the laws are different from country to country? Even if a particular country is able to identify a particular technological platform say, google or Facebook as the source of a crime, it is often difficult to act against them as permission is needed from the parent companies that are usually based in the US and who are often loathed to permit such intrusion or intervention. Even in the US, there can be difficulties as was evident in the 2015 San Bernardino shooting. At the same time the fear of the 'Big Brother Syndrome' had led the public to fear greater regulation of the ICT technologies by governments, thereby exacerbating tensions between rights of citizens and security concerns of governments.

Added to this, there is also the discussion on how many covert resources to develop to manage the threat and the fear that this may be abused for political purposes. Many societies are also loathed to surrender their rights to the government for fear that their privacy and rights will be abused and undermined. At the same time, it is also a truism that not all radicalization takes place through the Internet and Social Media. Increasingly, people are connected with one another and the person-to-person dimension of radicalization cannot be ignored. Hence, while technology is an important game changer, yet it is not the only game in town as other dimensions of radicalization also needs to be taken cognizant of, especially off-line.

References

[1] Ifueko Omoigui Okauru, "Identify and explain any five new ways that information and communication technology can be used to enhance academic work in the University of Ghana," College Workouts, vol. 29, 2012, Available at https://collegeassignments.wordpress.com/2012/10/29/identify-and-explain-any-five-new-ways-that-information-and-communication-technology-can-be-used-to-enhance-academic-work-in-the-university-of-ghana/.

[2] Indonesia is now top country for cybercrime, The China Post, 22 October 2013.

[3] Cybercrime Threat a Growing Concern: Police, The Jakarta Globe.

[4] Ibid.

[5] Brata Adisurya, "Cyber Terrorism di Indonesia". Available at https://www.academia.edu/11343439/Cyber_Terrorism_di_Indonesia; "Dosen Unisbank Ditangkap", Suara Merdeka, 24 August 2006.

[6] Mbai Ansyaad, in The New Dynamics of Terror Networks in Indonesia, pp. 38–39, BNPT, Indonesia, 2014.