THE THREAT OF CYBERTERRORISM AND THE APPLICABILITY OF THE CONVENTION OF CYBERCRIME

Sonny Zulhuda

Associate Professor and Indonesian Researcher, Ahmad Ibrahim Faculty of Laws, International Islamic University, Malaysia.

The proliferation of information and communications technology, merged with the increasing amount of big data and interconnectivity, turns out to be a deadly combination when it comes to the threat of terrorism. Just like any industry that grows up with the new technologies, criminals and terrorists would certainly make use of the sophistication of the Internet, mobile gadgets and artificial intelligence in order to launch their terrorist agenda. This is indeed the new challenges faced by the global community.

Nah Liang Tuang of Singapore-based S. Rajaratnam School of International Studies reckons that this technological advancement is a two-edged sword: One edge for a defence, the other for an offence. Technologies like smart-phone encryption, internet of things, and the ubiquity of computer networks in the military and vital public services create mixed outcomes such as facilitating defensive military mobilization while also incurring potential cyber-threats and cyber vulnerabilities. With this background, this short article aims to analyse the nature and scope of cyberterrorism and the latest development on the international initiative to provide legal countermeasures to this global security threat. Special attention will be attached to the Convention of Cybercrime.

The Risk of Cyberterrorism

The threat of cyberterrorism is a reality. In the Global Risks Report 2019 issued by the World Economic Forum, a lethal combination of large-scale cyber-attacks and a large-scale terrorist attack, representing geopolitical and technological risks respectively, continues to exist. The report describes large-scale cyber-attacks or malware such as those attacks that cause large economic damages, geopolitical tensions, or widespread loss of trust in the internet. Meanwhile, large-scale terrorist attacks mean those individuals or non-state groups with political or religious goals that aim to inflict large-scale human or material damage to their target.

A terrorist's use of the internet may also have other debilitating impact. In the same WEF report, the risks of terrorist attack were found to have a link of threat with other risks such as critical information infrastructure breakdown and the risk of launching of weapons of mass destruction. This is true because today we live in an interconnected world where more and more vital infrastructures are being digitized and relying on data infrastructure.

Furthermore, cyberterrorism becomes increasingly popular due to its ease and affordability. Terrorists do not have to get expensive conventional weapons and bring them to intended site physically. They are not restricted by time or space: attacks can be launched virtually from anywhere at any time. This fact is exaggerated by the superior level of anonymity offered by the computer networks and the Internet that allows the terrorists to hide behind the veil of technology. The impact can be huge, depending on what target is aimed at. The modus operandi is ranging from spreading logic bombs to Trojan horses, from worms to viruses, and from denial of services to network intelligence, etc.

Definition and Scope of Cyberterrorism

So, what is cyberterrorism? A computer misuse that disrupts the non-essential services is at most a costly nuisance and is not cyberterrorism. But serious or continuous cyber-attacks against nation's critical infrastructures such as those of medical services, key government agencies or the military bases can potentially undermine the resilience and reliability of the information systems wholly or substantially, and may in turn coerce the public and cause fear and anxiety.

Furnell and Warren (1999) define cyberterrorism as the use of cyberspace by terrorist groups, indicating a transition from traditional terrorism that depends on materialistic means to modern terrorism that relies more on invisible technologies. In a narrower sense, Lewis (2002) defines it as the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population.

From the above definition, one can describe cyberterrorism in two categories: One is where the "cyber-threat" element is crucial, namely an attack that targets, interrupts or cripples cyber or computer systems, which in turn would cause fear so as to further propagate their initial political or ideological agenda. This includes attacks to the military cyber-based systems or otherwise to a country's critical information infrastructure. In short, the cyber system is made as the target of the attack (Figure 1).

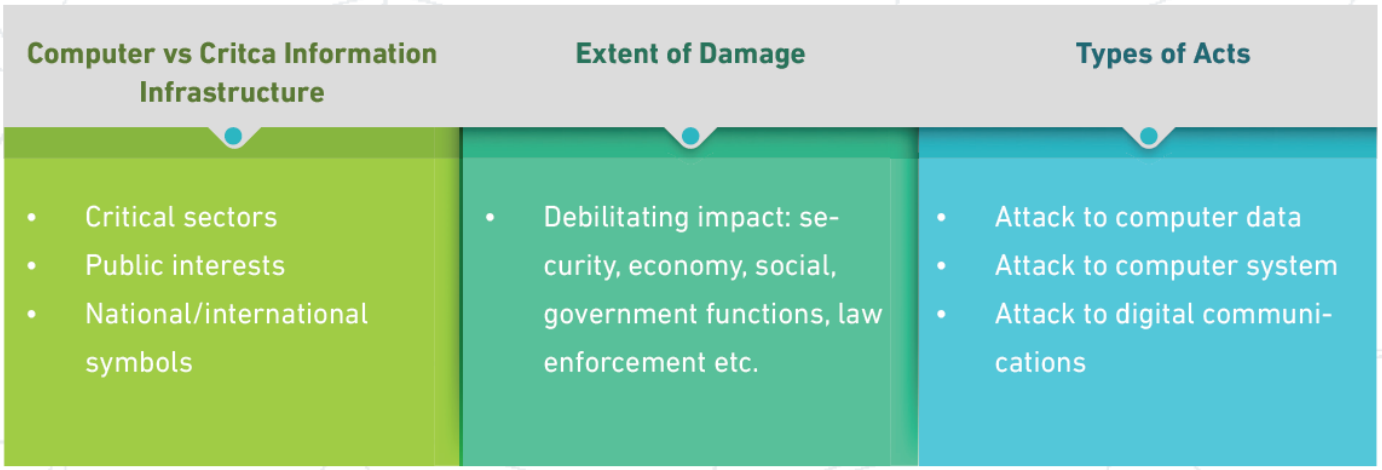

Figure 1: Scope of Cyberterrorism Category 1 – Attack to the system

The second category of cyberterrorism is where the cyber system is made as a medium of the attack. This is when the Internet or any information and communications systems (mobile gadget, IoT, Artifical intelligence, big data, encryption, robotic software, etc.) are utilized by terrorists for the purpose of planning, preparing and launching terrorist attacks. Grabosky (2007) describes how extensive information technology has been used: as a means to facilitate terrorism, including the hacking for intelligence; encrypted terrorist communications via the web; propaganda, i.e. bypassing journalistic editing and government censorship; psychological warfare, by generating anomalous pattern of traffic, giving a false impression that an operation may be imminent; fund-raising and recruitment; distant training, e.g. of attack technique and skills, training manual publication, weapon making manual (Figure 2).

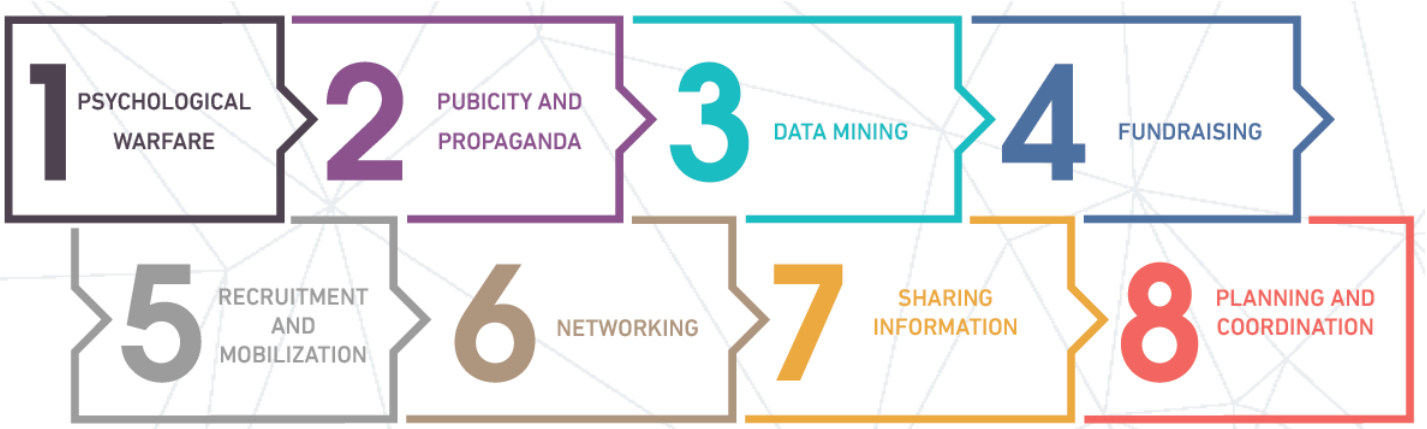

Figure 2: Types of Cyberterrorism Category 2 – Facilitated by the system

In Malaysia, the emergence of this second category of cyberterrorism activities has increased in the past decade. Prosecutions were brought under the country's Penal Code. Provisions under ss. 130C-130J enlist various acts that were committed in pursuance to terrorist acts, e.g. recruiting persons to be members of terrorist groups or to participate in terrorist acts; providing training and instruction to terrorist groups;

receiving training from terrorist groups and persons committing terrorist acts; inciting, promoting or soliciting property for the commission of terrorist acts; directing activities of terrorist groups; and soliciting or giving support to terrorist groups.

The International Initiatives to Address Cyberterrorism

Needless to say, cyberterrorism is a global risk and a global problem which requires a global solution. The then United Nations Secretary-General Ban Ki-moon said that the Internet is a prime example of how terrorists can behave in a truly transnational way. In response, states need to think and function in an equally transnational manner. In line with this observation, despite local laws and policies on cyberterrorism, we need to respond to this global risk with a synergized multinational approach. In this work we would assess the initiatives taken at the international level to address the threat of terrorism.

In 2012, the United Nations Office on Drugs and Crime (UNODC), in collaboration with the United Nations Counter-Terrorism Implementation Task Force, had released a working report relating to cyberterrorism. The UN Agency recognizes that despite international recognition of the threat posed by terrorists' use of the Internet in recent years, there is currently still no universal instrument that specifically addresses this pervasive terrorist activity. Adding to the cause of concern is the fact that there is limited specialized training available on the legal and practical aspects of the investigation and prosecution of terrorism cases involving the use of the Internet. Therefore, UNODC aims to develop resources on counter-terrorism and cybercrime for combating this evolving threat.

UNODC stresses that there are few factors necessary in outlining the global response of counter-terrorism measures, including: (1) Common policy and legislative frameworks; (2) Investigations and intelligence gathering; (3) International cooperation; (4) Prosecution; and (5) Private sector cooperation. All these primary factors are nevertheless dependant on the common commitment among countries to address and counter terrorism threats both within and beyond their national borders. How much are we ready for that? The fact is, until today there is no general convention that specifically addresses cyberterrorism.

The Convention of Cybercrime

Expectation has prolonged on the Convention of Cybercrime to fill the gap, though there is still much to do. When officially signed in 2001, the Convention itself was convened without citing terrorism offences as the scope of the treaty. It was initially meant to harmonize the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime, such as offences to the confidentiality, integrity

and availability of data. On top of that, the Convention also aims at setting up a fast and effective regime of international co-operation on countering cybercrime.

In response to this, the Cybercrime Convention Committee (T-CY) released in 2016 a guidance note relating to the cyberterrorism aspects by the Budapest Convention. The document addresses how the articles of the Convention could apply to terrorism. Therefore T-CY declares that "the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law". This additional note under the Convention is timely. In the wake of increasing threat of cyberterrorism, it is made clear that the cybercrimes set out in the Convention can indeed be perpetrated as acts of terrorism, to facilitate and support terrorism.

The Note further highlights that even though this Convention is not a treaty that is focused specifically on terrorism, it is however argued that the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate or support terrorism, including financially, or as preparatory acts. In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

For example, under the Convention, each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures for the purpose of specific criminal investigations or proceedings. Furthermore, such powers and procedures apply not only to the specific cybercrime offences as mentioned in the Convention, but also to "other criminal offences committed by means of a computer system". Therefore according to the 2016 Guidance Note, this would arguably extend the applicability of the Convention of Cybercrime to any terrorism offence as long as it is perpetrated by means of a computer system.

With this extension, one can argue that being a party to the Convention would help a country in addressing cyberterrorism in their own jurisdiction, noting that such country will be eligible to the mutual assistance and cooperation between member countries. First, Parties (to the Convention) shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Secondly, it also means that Party to the Convention will obtain its fair share to the international cooperation. Accordingly, the parties shall co-operate with each other to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. And the Party would be allowed to get mutual assistance even in the absence of applicable international agreements between countries.

Conclusion

It is concluded here that Cyberterrorism is a new form of terrorist acts, often having a more debilitating impact, but yet has been largely spared by many jurisdictions' policy and legislations.

Cyberterrorism is a global risk that requires a global response. We need a common policy and legislative framework setting minimum standard of laws and best practices. A concerted effort for information sharing and intelligence gathering is necessary. An international cooperation on investigation and prosecution, as well as a public-private cooperation would be critical.

One important global instrument at play is the Convention of Cybercrime, being the only international convention on matters relevant to cyberterrorism. Though the Convention does not specifically address cyberterrorism, yet it is worded in such a way as to extend it to the threats of terrorists, hence cyberterrorism offence. The best response still, would be to further amend the Convention and insert more specific cyberterrorism offences. However, the biggest challenge is arguably on how to get more countries involved to make it a more global and international instrument.