COMPUTER LAW & SECURITY REVIEW 32 (2016) 495–512

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Preventing intangible technology transfer (ITT) on the Internet and telecommunications for bioterrorism through Malaysia's Strategic Trade Act 2010 (STA 2010)

Marina Abdul Majid [a,b,*], *Azizan Baharuddin* [c], *Lee Wei Chang* [d]

[a] *School of History, Politics and Strategic Studies, National University of Malaysia (UKM), Bangi, Selangor 43600, Malaysia*
[b] *Department of Science and Technology Studies, Faculty of Science, University of Malaya (UM), Kuala Lumpur 50603, Malaysia*
[c] *Institute of Islamic Understanding Malaysia (IKIM), 2, Jalan Langgak Tunku, Kuala Lumpur 50480, Malaysia*
[d] *Centre of Research for Computational Sciences & Informatics for Biology, Bioindustry, Environment, Agriculture and Healthcare (CRYSTAL), University of Malaya (UM), Kuala Lumpur 50603, Malaysia*

Keywords:
Intangible Technology Transfer (ITT)
Strategic Trade Act 2010 (STA 2010)
Export control
Biological and Toxin Weapons Convention (BTWC)
Resolution 1540
Bioterrorism

A B S T R A C T

Malaysia's Strategic Trade Act 2010 (STA 2010) was drafted to address export controls and associated trade controls such as transit, transhipment and brokering in the fulfilment of the Biological and Toxin Weapons Convention (BTWC), Chemical Weapons Convention (CWC), Non-Proliferation Treaty (NPT) and the United Nations Security Council (UNSC) Resolution 1540, which broadly address the proliferation of nuclear, biological and chemical weapons. Terrorists have been known to utilise websites and emails to place manuals, instructions, blueprints and other documents, known as Intangible Technology Transfer (ITT), to incite and encourage their peers to create biological weapons; subsequently, to launch an attack of bioterrorism. Simultaneously, terrorists may camouflage their identity and attend oral and visual exchanges such as teleconferences, virtual meetings and skills training sessions that disseminate relevant information on biological weapons. This makes it possible for terrorists who already possess some background knowledge of biological weapons to further their interests in creating these weapons. The objective of this study is to analyse Malaysia's STA 2010 concerning relevant provisions that are able to address the threat of ITT over the internet and telecommunications by terrorists in the context of disseminating knowledge of biological weapons to perpetuate bioterrorism. The results show that the provisions of Sections 2, 4, 9 and 10 of STA 2010 are relevant in addressing the ITT of individuals using the internet to encourage creating biological weapons abroad by involving extraterritorial jurisdiction, extradition and mutual assistance in criminal matters. This study concludes that Malaysia's Ministry of International Trade and Industry (MITI) and the Malaysian Communications and Multimedia Commission (MCMC), implementers of the STA 2010, must deliberate on these unclear matters and draft detailed guidelines to direct Malaysian researchers and academics, learning from the examples of other countries.

* *Corresponding author.* School of History, Politics and Strategic Studies, National University of Malaysia (UKM), Bangi, Selangor 43600, Malaysia. Tel.: +60 03 8921 5824; fax: +60 03 8921 3290.
E-mail addresses: marina76@ukm.edu.my; mabdulma@hotmail.com (M. Abdul Majid).
http://dx.doi.org/10.1016/j.clsr.2016.01.008

1. Introduction

In this modern, ever-evolving era of telecommunications, there is an emerging trend concerning terrorists' quest for knowledge to create biological weapons for bioterrorism. This can be done through information acquired from the internet, through email communications and numerous websites of Islamic extremists based within a country or abroad. Telecommunications itself is understood as 'any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems relevant to the communication of emails and websites.'[1] For the purpose of this study, focusing on Malaysia's Strategic Trade Act 2010 (STA 2010), a definition of biological weapons from STA 2010 is understood as 'any microbial or other biological agents or toxins, whatever their origin or method of production of type, and in quantities that have no justification for prophylactic, protective or other peaceful purposes and weapons, equipment or means of delivery designed to use biological agents or toxins for hostile purposes or in armed conflict.'[2] Biological agents in the STA 2010 means 'any microbial, micro-organism, virus or infectious substance derived from them naturally or artificially, as well as, their components and whatever method of production.'[3] The 'deliberate release of viruses, bacteria, or other germs (agents) used to cause illness or death to people, animals or plants was defined by the United States (US) Centres for Disease Control and Prevention (CDC) as bioterrorism.'[4] In the STA 2010, a software programme is defined as 'a collection of one or more programmes or micro-programmes recorded, stored or embodied in any device.'[5]

Terrorist and spies' acquisition of knowledge for creating biological weapons raises the need to impose export controls. Export controls are a 'set of laws, policies and regulations that govern the export of sensitive items for a country or company.'[6] The imposition of export controls is needed to safeguard the transfer of information, commodities, technology and software considered strategically important to a country to protect national security, economic or foreign policy concerns. Export controls are implemented to ensure valuable information, commodities, technology and software are not acquired by terrorists or other countries for misuse, threatening a country's defences or serving as an economic and technological competitor.

More importantly, export control raises the concern of Intangible Technology Transfer (ITT) that is 'the transfer of technology through intangible means: electronic communications, fax, oral instruction or training.'[7] Gruselle and Meur[8] indicated that ITT can be in two principle forms; namely, the transfer of knowledge as technical assistance and the transfer of technical data. In Malaysia's STA 2010, a definition of technical assistance is provided in Section 2 to include 'instructions, skills, training, the provision of working knowledge and consulting services which may involve the transfer of technical data.'[9] Furthermore, technical data in Section 2 encompass 'blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions in print or electronic format.'[10] Additionally, Section 2 defined technology as 'information and data in any form for the design, development, production or use of another item and includes technical data, technical assistance and software.'[11] The STA 2010 also exempts any basic research put in the public domain of the internet from export controls of ITT. While the STA 2010 itself does not define public domain, the Strategic Items List defines 'in the public domain' to mean technology or software which has been made available without restrictions upon its further dissemination.[12]

Malaysia has not been spared, playing a host to Islamic extremist websites periodically, as highlighted by scholars such as Weimann[13] and Thomas[14] regarding the Al-Neda website hosted by a Malaysian company called Emerge Systems. Bergin et al.[15] further indicated that the *Forum Al-Tawbah* in 2008 was registered in Shah Alam, Malaysia; and Davis[16] referred to the Al-Ansar Al-Islam website, famous for showing the beheading video of Nicholas Berg in 2004, as being hosted by Malaysia's Acme Commerce. Not only is Malaysia affected, but also the

[1] National Communications System Technology & Standards Division, *Telecommunications: Glossary of Telecommunications Terms* (General Services Administration Information Technology Service 1996) <http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm> accessed 8 January 2015.

[2] Strategic Trade Act 2010 (Malaysia), s 2.

[3] Strategic Trade Act 2010 (Malaysia), s 2.

[4] Centers for Disease Control and Prevention, United States, 'Bioterrorism Overview' (2015) <http://emergency.cdc.gov/bioterrorism/overview.asp> accessed 1 July 2015.

[5] Strategic Trade Act 2010 (Malaysia), s 2.

[6] Institute for Science and International Security, Washington, United States, 'E-Book Glossary' (2015) <http://exportcontrols.org/glossary.html> accessed 25 September 2015.

[7] Bruno Gruselle and Perrine Le Meur, 'Technology Transfer and the Arms Trade Treaty- Issues and Perspectives' (2012) Researches & Documents No. 02/2012, 8, <https://www.frstrategie.org/publications/recherches-documents/web/documents/2012/RD_201202.pdf> accessed 1 July 2015.

[8] ibid 8.

[9] Strategic Trade Act 2010 (Malaysia), s 2.

[10] Strategic Trade Act 2010 (Malaysia), s 2.

[11] Strategic Trade Act 2010 (Malaysia), s 2.

[12] Ministry of International Trade and Industry (MITI), Malaysia, 'Strategic Items List' (2011) <http://www.miti.gov.my/miti/resources/STA%20Folder/PDF%20file/Strategic_Items_Under_The_STA_2010.pdf> accessed 25 September 2015.

[13] Gabriel Weimann, 'The Psychology of Mass-Mediated Terrorism' (2008) 52 American Behavioral Scientist 69, 75 <http://abs.sagepub.com/content/52/1/69.full.pdf> accessed 23 December 2014.

[14] Timothy L Thomas, 'Al Qaeda and the Internet: The Danger of "Cyberplanning"' (2003) 23 Parameters 112, 115 <http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf> accessed 2 December 2014.

[15] Anthony Bergin, Sulastri Osman, Carl Ungerer and Nur Azlin Mohamed Yasin, 'Countering Internet Radicalization in Southeast Asia' (2009) Australian Strategic Policy Institute 22, 6 <http://cleanitproject.eu/files/95.211.138.23/wp-content/uploads/2012/07/2009-Internet-radicalisation-Sout-East-Asia.pdf> accessed 5 December 2014.

[16] Benjamin R Davis, 'Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance' (2006) 15 Common Law Conspectus 119, 134–135.