IS CYBER CRIME REIGNING ON A NO MAN'S LAND?

By
National ICT Security and Emergency Response Centre (NISER)

INTRODUCTION

Cyber space is a virtual space that has become as important as real space for business, politics, and communities. Malaysia's commitment in using Information and Communication Technology (ICT) as reflected by the investment in the Multimedia Super Corridor (MSC) and its Flagships increases our dependency on cyber space. However, this dependency places Malaysia in an extremely precarious position because cyber space is vulnerable to borderless cyber attacks.

Cyber space, as it stands today, gives rise to both positive and negative consequences. For negative consequences, the ingredient of this digital soup is so vague that many refer to it as the dark sides of technology and that cyber criminal currently have the upper hand over law enforcement efforts. The applicability and effectiveness of our existing laws need to be constantly reviewed to face the risks coming from the cyber world.

DEFINITION OF CYBER CRIME

The Oxford Reference Online defines cyber crime as crime committed over the Internet. *The Encyclopedia Britannica* defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology. (www.crime-research.org/library/Cybercrimimal.html)

Cyber crime could reasonably include a wide variety of criminal offences and activities. The scope of this definition becomes wider with a frequent companion or substitute term "computer-related crime." Examples activities that are considered cyber crime can be found in the *United Nations Manual on the Prevention and Control of Computer-Related Crime.* The manual includes fraud, forgery, computer sabotage, unauthorised access and copying of computer programs as examples of cyber crime. (www.uncjin.org/Documents/EighthCongress.html)

Malaysia was amongst the first few countries in the world to introduce cyber laws. An example of such cyber is the Computer Crimes Act 1997. This cyber law addresses and looks into areas of cyber crime activities.

STATISTICS ON CYBER CRIME MAY NOT BE REAL

Statistics may show the trend on cyber-crime activities but are not a reliable source to determine the actual position of the computer crime rate. Criminologists use the term "dark figure" to describe the undetermined actual position which refer to those

undetected computer crimes activities. Several contributing factors below may explain why it is called “dark figure”.

First, the fast operational speed of today’s computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity. Third, once criminal activity has been detected, many businesses are reluctant to lodge a report due to fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions.

CROSS-BORDER JURISDICTION

Why does the cyber space have no owners, is lawless and illimitable? One of the reasons is the fact that Internet is a free-flow information channel. This fact has however created a new problem which concerns jurisdictional issues. For example, Dmitry Skylyarov a Russian software programmer who provided software used to crack e-books was jailed after he entered the United States. His action is not a crime in his homeland but violates US copyright laws.

The jurisdiction issue in a computer mediated communication is easy to determine, particularly if the victim is located in another country. Therefore, whenever a crime is committed via cyberspace, the court will face a problem in deciding which country’s jurisdiction does the committed crime fall under. Though courts and lawmakers have constantly echoed that there is a global revolution looming on the horizon, the development of the law in dealing with cross-border jurisdiction is still in its infancy.

The ‘infant’ law must be further nurtured and developed to become a full-fledge set of cyber laws that lucidly defines a country’s jurisdiction whenever a cyber crime is committed. That law should for example address whether a particular event in cyberspace is governed by the laws of the state or country where the offence is committed, or by the laws of the state or country where the target is located, or perhaps governed by all of these laws.

CYBER CRIME AND TECHNOLOGY

As technology in ICT becomes more advanced, law enforcement agencies must provide their computer crime investigators with the technology required to conduct complex computer investigations.

Besides access to technology, law enforcement agencies must also be given forensic computer support as many computer crimes leave “footprints” on the computer as well as on the Internet. Most prosecutors also lack the training and specialization to focus on the prosecution of criminals who use computer-based and Internet system as a means of committing crimes. Thus, they must have a working knowledge of computer-based and Internet investigations if they are to handle these crimes effectively.

The enforcement and jurisdiction agencies must be able to understand and comprehend ICT security technologies reasonably well or otherwise they may be overwhelmed by the technical details and be manipulated by lawyers and expert witnesses from both prosecution and defence. A good example is a recent case in UK where a teenager was acquitted after being charged in court for Distributed Denial of Service (DDOS) attack that crippled the Port of Houston, a US web-based computer system.

The defendant claimed that the attack from his PC was a result of a Trojan that enabled attackers to take control of his PC and performed an attack to a target in the US. The defendant further claimed that the Trojan was able to wipe itself out - without presenting any evidence. It was also interesting to note that although the expert witness has found the attack tools but without a trace of Trojan infection, he failed to convince the jury.

The outcome of this case is irrational and will have a major impact on the way which cases will be dealt in the future. The relevant agencies must be constantly trained to educate themselves with the Internet and computer-based evidence. Continual awareness and training is an absolute necessity in order to understand and comprehend ICT security technologies.

CONCLUSION

If businesses can make great use of these unifying measures, so can the criminals. Inspire by this perception and also due to the emerging international crime-related issues, there is a possibility of governments from all over the world to unify in enacting a set of international laws accepted by most, if not all. To ensure comprehensiveness, such enactment shall take into consideration cyber activities that are beyond traditional areas.

Criminals have adapted the advancements of computer technology to further their own illegal activities and these inventiveness have however, far out-paced the ability of law enforcement agencies to react effectively. Therefore, within the law enforcement agencies, a set of rules must be developed to address the various categories of computer crime. As such, investigators will know what and which materials to search and seize, the electronic evidence to recover, and the chain of custody to maintain. Only then we can truly enforce law and order into “no man’s land”.