The Need for More Legal Materials for Better Understanding of Malware and Badware Threats in Malaysia

Article *in* Mediterranean Journal of Social Sciences · January 2017

DOI: 10.5901/mjss.2017.v8n1p134

CITATIONS
0

READS
48

1 author:

Rizal Rahman
Universiti Kebangsaan Malaysia
39 PUBLICATIONS **18** CITATIONS

SEE PROFILE

The Need for More Legal Materials for Better Understanding of Malware and Badware Threats in Malaysia

Rizal Rahman

Associate Professor, Faculty of Law, Universiti Kebangsaan Malaysia
Email: noryn@ukm.edu.my

Doi:10.5901/mjss.2017.v8n1p134

Abstract

This article examines the literature surrounding malware and badware in Malaysia. While there have been numerous technical literature on the subject matter, there is no sufficient materials to cater to the legal understanding. The articles seeks to find the reasons behind this problem and propose a practical approach to it.

Keywords: *malware; badware; cybercrimes; Malaysia*

1. Introduction

The dissemination of traditional malware and badware, namely viruses, worms and trojans (just to name a few), particularly by way of sneakernetting, has been in practice for almost thirty years since the first computer virus, "Elk Cloner", was detected "in the wild" (perceived outside a controlled environment) in 1982 (Sullivan, 2005). That was the case when the development and dissemination of computer viruses were perceived outside a controlled environment. However, the history of virus development in a controlled environment, for example in a computer lab, can be traced back to the first generation of computers in the 1960s. Even earlier, in 1948, Turing (1948) already envisaged the possibility of self-propagating computer programs. However, the term "computer virus" was only made popular in 1984, followed by the first PC virus, "(c) Brain" in 1986. The Elk Cloner and (c) Brain detection has sparked voluminous legal (and technical) literature on the danger of malware and badware, especially after the first "Morris worm" incident in 1988 and the Black Baron case in 1990 (Lilley, 2002).

The Morris worm was created by Robert Morris who released a self-replicating bit of code which caused excessive load on VAX and Sun machines until users were not able to log on. He was tried for violating the Computer Fraud and Abuse Act of 1986 (United States) and he became the first person convicted under the Act. The Black Baron (Christopher Pile) was the first person convicted under the CMA for writing and disseminating Smeg, a virus toolkit, Pathogen and Queeq viruses, and inciting other people to spread computer viruses (Kizza, 2009). But the real impact of malware and badware was only felt when the Melissa virus was released in 1999, infecting millions of computers worldwide (Turrini & Ghosh, 2010).

The main objective of this article is to propose a practical approach to be adopted by legal authors in Malaysia in the write-ups about malware and badware threats. It is a library-based work where the author examines various sources related to the issue.

2. Malware, Badware and Legal Literature

The abundance of literature on malware and badware does not mean that the issues are settled. Durham (1982) already pointed this out:

> *"Any analysis of the impact of the computer on law is hampered by the same problems that afflict general efforts to keep pace with the computer revolution itself: the incredible proliferation of scholarly literature on the subject and the rapidity with which the literature, like the underlying technology,* ***becomes obsolete****." (Emphasis added).*

It follows that previous literature is superseded every time a new generation of malware and badware is born. This is further compounded by the fact that Malaysia has no comprehensive legal literature on malware and badware. In fact, Malaysia has too few text books which deal specifically with cybercrimes. Most that do exist are quite descriptive and

repetitive in nature. None of the literature analyses the malware and badware invasion and integrates it in arguments in the way submitted in this research. Damage, deception and trespass are discussed in the literature, but only in the context of cybercrimes in general, not from the perspective of malware and badware invasion. The focus has been on the elements of the offence of damage, deception and trespass committed virtually, rather than a determination of the efficiency of the law regulating those offences.

The reason why the Malaysian literature only focus on the general cybercrimes is because of the seemingly limited nature of the Computer Crimes Act and malware and badware. The Computer Crimes Act has always been the main subject of criticisms in the literature on the ground that the provisions are not expansive enough to cater to all areas of cybercrimes, while the Penal Code has always been viewed as too traditional, outdated and not viable to handle cybercrimes. This is further compounded by the fact that the Computer Crimes Act has never been amended since it was passed in 1997. However, these criticisms are levelled on the premise that a new set of laws is required, rather than making use of existing laws by applying a new way of interpretation.

It has been argued in the Malaysian Public Sector Management of Information & Communications Technology Security Handbook (2001) that:

> *"Telecommunications fraud, computer-related crime incidents, investigations and computer forensics involve sciences affected by many external factors, such as continued advancements in technology, societal issues and legal issues. Most of the cases are esoteric in nature and there have been very few prosecutions and even fewer convictions being made. This is because of the many grey areas to be sorted out and tested through the courts. Until then, system attackers will have an advantage and computer abuse will continue to increase."*

The above perception is also held in other countries, as far as their criminal codes are concerned. In many cases, such a perception derives its origin from Moor's (1985) influential theory of "policy vacuums" - a situation where new possibilities and circumstances created by computer technology do not seem to fit within existing policies and laws. He argued that even if attempts are made to expand the policies and laws to cover "new possibilities" and circumstances, the problem of "conceptual muddles" awaits. He further stressed that "conceptual muddles" is a situation where computer technology presents confusion as to what legal and ethical concepts could be applied to such possibilities and circumstances.

Moor's theory has become so influential that many authors directly or indirectly resort to it to defend the need for descriptive legal provisions on types of cybercrimes in lieu of the existing "traditional" legal provisions. Brenner (2007) argued that "it became equally apparent that the 'internal' laws nations had adopted to deal with cybercrime were insufficient to deal with externally based activity". Clifford (2006) remarked that "inadequate domestic legislation, combined with the failure of unanimous global cooperation, creates a gap in enforcement that provides safe havens for targeted conduct". In the international arena, all arguments on jurisdiction over the cross border nature of cybercrimes tended towards the same conclusion over and over again: the need for harmonisation of laws among countries. Yar (2009) pointed out that the move towards harmonisation is in "a relatively nascent stage" but Kshetri (2010) argued that the "collaborations and cooperation among law-enforcement agencies in different jurisdictions have been insufficient". In this regard, Feick and Werle (2010) have remarked:

> *"The limits of enforcement in a network that easily crosses borders are obvious. A promising response to these limits would be the international harmonisation of regulation. But here the above-mentioned differing national cultural values and norms, as well as distinct legal traditions, make it extremely difficult to reach international agreements - and they are time-consuming if reached at all."*

This debate on harmonisation has led to the cynical argument that "to hope for a comprehensive, internationally agreed and cross border enforceable set of laws and penalties to curtail cyber crime, *is fiction*" (Solms, 2010). (emphasis added).

There has not been much exploration by Malaysian authors on the existing laws relevant to the subject despite the fact that the threat posed by malware and badware has caused damage and loss to the Malaysian public. This is a total contrast to non-Malaysian legal literature, in particular materials written for the United States and European market. A study in 2007 revealed that from 1974 until 2006, the standard annual publication rate on cybercrimes in general was 30.8%, with a considerable increase starting from 2003 (Lu, Jen & Chang, 2010). This involved 121 journals, around 2.41 papers per journal.

However, as the impact of the subject matter of the research is felt globally, the scarcity of Malaysian materials does not mean that it is a dead end for any research on the subject. In building up a research on the matters, all non-

Malaysian materials relevant to the experience of the impact should be thoroughly considered to fit the local analysis. While doing this, technical literature on malware and badware should also be referred to. This has to be done on the ground that the technical literature best describes the malware and badware invasion on a first-hand basis.

While referring to the technical literature, one should never fail to acknowledge that the literature contains arguments not currently practicable by legal measures. It is understood that technology is moving very fast, hence laws must also be developed at the same pace. However, to what extent is that possible? Wolf (2009) drew a good analogy for this. He looked at criminal technology of the past as Crime 1.0 and the present one as Crime 2.0. During the Crime 1.0 era, which began in 1908 after Henry Ford created affordable cars for the average citizens of the United States, criminals became difficult to track through their use of newly bought vehicles, leaving the legal officers behind in their old cars and horses. The authorities learned to combat this by purchasing better cars and sending officers to driving lessons. A century later, Crime 2.0 era started when criminals, equipped with high tech gadgets, used computers as their vehicles of crimes. They engaged in new modus operandi. Their techniques get better from year to year, month to month, and the "time and again" feature becomes proximal (Wall, 2007). As new technology comes along, it operates as a benefit or challenge to the police and criminals, depending on who manages to get hold of the technology first. Hence legal authorities need to stay ahead of the state-of-the-art criminals.

Despite the fact that laws should always be at the vanguard, and while law has to be concerned with the legal effects of malware and badware at individual and societal level, the legislature has to avoid too much specification. While descriptive measures are indeed necessary in certain circumstances, the way they are drafted should not be too specific that it is likely that they may be obsolete in a matter of a year or two. For example, Kirby (2006) referred to the "technology-specific prohibitions" in the Washington anti-spyware statute and considered them as provisions which guarantee a technological avoidance as they are too specific and not "technology-neutral".

On the other hand, if laws are over-inclusive or too general, they may lead to numerous interpretations, which may then lead to doubt in their application. Therefore a balance has to be carefully struck between narrowness and breadth in the search for law that is theoretically and practically efficient. But how is that balance to be struck? The flow of progress in technology is not as humanly paced as law making. This is because law, in contrast to technology, is not passed within seconds, nor is it supposed and expected to be of a trial-and-error nature. Unlike computer experts who do not have to wait long for a brand new technology to be released, legal professionals can only wait and predict, albeit sometimes prematurely, the possible legal measures to be taken by their respective legislatures. This has created a gap between the two distinct but interrelated literatures. Schultz (2004) already warned about the disparity between the two disciplines:

> *I fear we tend to glorify computer scientists who create new security tools or develop new encryption algorithms and too often ignore social scientists who have much to offer in our war not only against worms and viruses, but also against computer crime itself.*

However, in many instances it is common to find legal ideas being mooted in the technical materials. This contribution by non-legal technical writers has sparked a new dimension as to how the legal community should realistically respond.

3. Recommendations and Conclusions

That is why legal authors in Malaysia need to adopt a different approach towards the Computer Crimes Act and the Penal Code: *analytical reinterpretation* for a better legal effect. It should always be remembered that although one is dealing with a fast evolving technology, the peril of "label oversimplification", where attempts are made to legally define almost everything, has to be taken into account as well (O'Neil (2001). There is no need to come up with "new" legislation every time a threat is felt, when there are actually ways for the threat to be handled by existing policies and laws. That option has not been favoured by many, especially those who adopt pro-Moor arguments, reflecting their fear of computer technology which they view as alien and incompatible with laws. Those arguments should nowadays be considered as orthodox and should no longer stand as technology is becoming integrated with daily life. "Conceptual muddles" were indeed just a perplexed theory in an era where lawyers and ICT professionals worked without sufficient regard to one another's respective fields. In facing more new technology to come, what is needed is the amalgamation of knowledge, not arguments based on laws alone without adequate understanding of technology and vice versa.

Otherwise another problem will arise: excessive criminalisation by legislating more than is needed. Sommer (2000) pointed out that:

> *"We should not expect much novel law, for at least two reasons. First, new technologies more often facilitate existing practices than generate new ones. Second, even new social practices are often well served by traditional legal devices."*

Howell (2007) also stated:

> *"Will the pace of legal changes always be behind technological developments? Yes, but in my view the correct pace is a "go slow" one. By the time a proposal has gone through the legislative process, the problem it seeks to address will have ripened into better definition. The better defined a problem is, the better policy makers are able to craft a narrow and circumscribed law to address the problem, while minimizing the risk of excessive breadth that could chill innovation and technological development."*

However, Hancock (2001) argued that:

> *"Developed commercial societies cannot afford to sit idly by in the hopes that ambiguous and often outdated laws can be reshaped to redress wrongs that were not contemplated by the original law's drafters. The drafting, implementation and eventual amendments to computer crime legislation, represent an essential response to a social imperative arising in the Information Age."*

It is important to respond to Hancock's argument by stressing that it is futile to interpret legislation solely on the intention of the legislature at the time it was passed, in relation to ICT technology. As Aquilina (2010) put it:

> *"…law can never catch up with fast and progressive technological change more often than not ending up reacting to something which has already become passe´ when a law is enacted to regulate that specific technology. On the contrary, the law should strive to be proactive and forward looking with regard to the technology sector."*

Hence, the rule of interpretation has to be based on the current development of ICT, provided that the wording of the statutes allows. While we do not neglect the intention of the legislature, interpretation should not be dependent on the intention alone. As for necessary amendments, the process should not take too much toll on the legislature. The process should instead be vested in the powers of delegated legislation which is less formal and convenient for immediate rule-making. The provision has to be followed by the addition of illustrations following the provisions to express its "new" additional effect.

References

Abu Bakar Munir & Siti Hajar Mohd. Yasin. (2010). *Information and communication technology law: State, internet and information: Legal and regulatory challenges*., Petaling Jaya: Sweet & Maxwell Asia.

Abu Bakar Munir. (1999). *Cyber law: Policies and challenges*. Kuala Lumpur: Butterworths Asia.

Ahmad Shamsul Abd. Aziz & Nurretina Ahmad Shariff. (2004). *Pengenalan kepada undang-undang pengurusan teknologi (Introduction to technology management law)*. Petaling Jaya: Pearson Prentice Hall.

Ahmad Shamsul Abd. Aziz, Khadijah Mohamed & Mazita Mohamed. (2007). *Undang-undang multimedia (Multimedia law)*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

AJ Surin. (2006). *Cyberlaw and its implications.* Subang Jaya: Pelanduk Publications.

Anis Suraya Abdullah (Ed.). (2009). *Fenomena jenayah siber (Cybercrime phenomena)*. Selangor: Penerbit Pinang.

Anita Abdul Rahim & Nazura Abdul Manap. (2004). *Jenayah berkaitan dengan komputer: Perspektif undang-undang Malaysia (Computer related crimes: the Malaysian legal perspective)*. Kuala Lumpur: Dewan Bahasa dan Pustaka.

Aquilina, Kevin. (2010). Public security versus privacy in technology law: A balancing act?" *Computer Law & Security Review*, 26, 130-143.

Brenner, S. W. (2007). The Council of Europe's Convention on Cybercrime. In Balkin, J. M., Grimmmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.), *Cybercrime: Digital cops in a networked environment*. New York: New York University Press.

Chichao Lu, Wenyuan Jen & Weiping Chang. (2007). Trends in computer crime and cybercrime research during the period 1974-2006: A bibliometric approach. Proceedings of the Intelligence and Security Informatics: Pacific Asia Workshop (PAISI) 244 at 246.

Clifford, R. D. (2006). *Cybercrime: The investigation, prosecution and defense of a computer-related crime*. 2nd ed. Durham: Carolina Academic Press.

Cohen, Fred. (1987). Computer viruses: Theory and experiments. *Computers and Security*, 6(1), 22-35.

Colton, K. W. (1979). *Police and computer technology: A decade of experience since the Crime Commission*. Washington: National Institute of Law Enforcement and Crimal Justice.

Daswani, N., Kern, C., & Kesavan, R. (2007). *Foundations of security: What every programmer needs to know*. Berkeley: Apress.

Durham, W. C., Jr. (1982). The modification of law under the influence of computer technology. *Am. J. Comp. L. Supp.*, 30, 601-619.

Feick, Jurgen & Werle, Raymund. (2010). Regulation of cyberspace. In Baldwin, R., Cave, M., & Lodge, M. (Eds.), *The Oxford handbook*

of regulation (pp. 523). Oxford: Oxford University Press.
Hancock, D. H. (2001). To what extent should computer related crimes be the subject of specific legislative attention? *Alb. L.J. Sci. & Tech.*, 12, 97.
Howell, B. A. (2007). Real-world problems of virtual crime. In Balkin, J. M., Grimmelmann, J., Jatz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.), *Cybercrime: Digital cops in a networked environment* (pp. 87). New York: New York University Press.
Izura Masdina Mohamed Zakri, Pek San Tay & Chew Li Hua. (2004). *Introduction to cyberlaw of Malaysia*. Kuala Lumpur: Advanced Professional Courses.
Kirby, C. A. (2006). Defining abusive software to protect computer users from the threat of spyware. *Computer L. Rev. & Tech. J.*, 10, 287.
Kizza, J. M. (2009). *A guide to computer network security*. Chattanooga: Springer.
Kroczynski, R. J. (2008). Are the current computer crime laws sufficient or should the writing of virus code be prohibited? *Fordham Intellectual Property, Media & Entertainment Law Journal*, 18, 817-866.
Kshetri, Nir. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. New York: Springer.
Lehtinen, R., Russell, D., & Gangemi, G. T. *Computer security basics*. 2nd ed. Sebastopol: O'Reilly & Associates.
Lilley, Peter. (2002). *Hacked, attacked & abused: Digital crime exposed*. London: Kogan Page.
Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) (2001). Malaysian Administrative Modernisation and Management Planning Unit, Putrajaya.
Mohd. Safar Hasim. (2002). *Mengenali undang-undang media dan siber (Understanding media and cyber law)*. Kuala Lumpur: Utusan Publications & Distributors.
Mohd. Shah A' Shaari & Abu Bakar Suleiman. (2006). *Jenayah siber: Apa anda perlu tahu (Cybercrime: What you need to know)*. Johor Baharu: ABS Tinta.
Moor, J. H. (1998). Reason, relativity and responsibility in computer ethics. *Computers and Society*, 28(1), 14-21.
Moor, J. H. (1985). What is computer ethics? Metaphilosophy, 16, 266-275.
Mueller, Milton. (2010). *Networks and states: The global politics of internet governance*. Massachusetts: MIT Press.
MyCERT CyberSecurity Malaysia Reported Incidents based on General Incident Classification Statistics 2015.
Nuth, M. S. (2008). Taking advantage of new technologies: For and against crime. *Computer Law & Security Report*, 24, 437.
O'Neil, Micheal. (2001). Cyber dilemma. *Brookings Review*, 28.
Schultz, Eugene. (2004). Worms and viruses: Are we losing control? *Computers & Security*, 23, 179.
Solms, Basie von. (2010). Securing the internet: Fact or fiction? In Camenisch, J., Kisimov, V., & Dubovitskaya, M. (Eds.), *Open research problems in network security: IFIP WG 11.4 International Workshop*. Berlin: Springer.
Sommer, J. H. (2000). Against cyberlaw. *Berk. Tech. L.J.*, 15, 1145.
Sullivan, Dan. (2005). *The definitive guide to controlling malware, spyware, phishing, and spam*. Realtimepublishers.
Szor, Peter. (2005). *The art of computer virus research and defense*. Upper Saddle River: Addison-Wesley.
Tavani, H. T. (2000). Defining the boundaries of computer crime: Piracy, break-ins, and sabotage in cyberspace. *Computers and Society*, 30(3), 3.
Turing, Alan. (1948). Intelligent Machinery, *Machine Intelligence*, 5, 3-23.
Turrini, Elliot & Ghosh, Sumit. (2010). A pragmatic, experiential definition of computer crimes. In Turrini, Elliot & Ghosh, Sumit. (Eds.), *Cybercrimes: A multidisciplinary analysis*. Berlin: Springer
Turrini, Elliot. (2010). Increasing attack costs & risks and reducing attack motivations. In Sumit Ghosh & Turrini, Elliot (Eds.), *Cybercrimes: A multidisciplinary analysis* (pp. 369-374). Berlin: Springer.
Wall, David. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity.
Wall, David. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.
Wolf, Ulf. (2009). Cyber-crime: Law enforcement must keep pace with tech-savvy criminals. [Online] Available: http://www.govtech.com (8 January 2009)
Yar, Majid. (2009). The internet and human (in)security. In Fagan, G. H., & Munck, Ronaldo. *Globalization and security: An encyclopedia* (pp. 247). Santa Barbara: Praeger Security International.
Zawiyah Mohammad Yusof, Hairudin Harun, Masnizah Mohd, Nazura Abdul Manap & Azizi Abdullah. (2007). *Teknologi maklumat & komunikasi: Etika, undang-undang dan sosial (Information technology & communication: Ethics, law and society)*. 2nd ed. Kuala Lumpur: McGraw Hill.