DE GRUYTER OPEN

Research Article

How the Legal Fraternity Should Respond to Modern Cybercrimes

Rizal Rahman

Associate Professor, Faculty of Law,
Universiti Kebangsaan Malaysia

Doi:10.5901/mjss.2017.v8n1p41

Abstract

This article examines the responses by the legal fraternity in the United Kingdom and United States towards modern cybercrimes, i.e. when cybercrimes are committed using malware and badware. While there have been attempts to cater to those crimes, there has been no viable mechanism yet. The articles seeks to find the reasons behind this problem and proposes a practical approach to it.

Keywords: *malware; badware; cybercrimes; United Kingdom; United States*

1. Introduction

Garrie and Komagome (2008), commenting on spyware (a form of malware and badware) came to the conclusion that there is no particular law in any country which has been able to hold up its expansion. This raises a question: Is something wrong with the cybercrime legislation? Clough (2010, p. 18) provides the following guideline:

> *"Where conduct is already criminalised in the offline environment, the question then becomes whether the law requires modification to ensure it may be prosecuted in the online environment. Rarely, if ever, would it be the case that conduct which may be prosecuted offline should not be criminal online. Conversely, where conduct is not criminalised in the offline environment, the question is whether technology has had such an impact on the nature of the conduct or its prevalence that it necessitates criminalisation. In such cases, the decision to criminalise is no different to criminalisation in the offline environment, and is subject to the same guiding principles."*

What can be derived from the above guideline is that one does not need to view technology as a barrier from applying existing law when the manipulation of the technology brings problems which could actually be handled by such law. However, the attitude of the legal community in the past was tainted with prejudice that law and technology were seen to be incompatible with one another.

2. The Responses so Far

The legal background towards the passing of the Computer Misuse Act 1990 has proven the existence of this sentiment. Looking at the history behind the introduction of the Computer Misuse Act 1990, the main reason for its passing was the principle put forward by the House of Lords in the 1988 case of *R v Gold & Schifreen (1988) 1 AC 1063*. The court held that the act of unauthorised access to a computer system did not constitute an offence under the existing criminal law. Lord Chief Justice Lane held that:

> *"The appellant's conduct amounted in essence ... to dishonestly obtaining access to the relevant Presiel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts. We express no view on the matter."*

While it is not wished to dispute the two decades old decision, it seems that the main reason behind the passing of the Computer Misuse Act 1990 was reluctance on the part of the judiciary and the English Law Commission to apply a

dynamic interpretation to the existing law at the time. Such reluctance was caused by public perception of the ICT environment as something "new". This judicial attitude had created panic in the legal arena as hackers would be deemed immune from law unless a new legislation was passed. Even the English literature of that era leaned towards the same timid sentiment, with the exception of the view of several authors like Bainbridge (1989) who argued that the existing legislation would be sufficient to handle cybercrimes. Lloyd (1988) however stressed that the "legislative action should not be long delayed". Dumbill (1990), commenting on the judicial decision of *Cox v Riley (1986) 83 Cr App R 54*, argued for a separate legislation and claimed that it was not fitting for the court to have applied the law of criminal damage in that case. His reason was that the Criminal Damage Act 1971 was not appropriate and was not originally intended by the legislature to deal with "the intricacies of sophisticated hacking techniques".

Despite the belief that the Computer Misuse Act 1990 would provide relief against modern cybercrimes, the technological reality has not been so. This has led to the demand for more amendments to be made to the Computer Misuse Act 1990. Fafinski (2006, p. 442) argued:

> *"The Computer Misuse Act 1990 was drafted with the laudable intention of providing flexibility to adapt to a rapidly evolving field of criminal behaviour; however, the nature of technological change went far beyond that envisaged in the late 1980s to provide situations that the Act could not reach."*

For example, there were still murmurs of discontent years after the Computer Misuse Act 1990 was passed in relation to whether the law of deception could be applied to computers. While Computer Misuse Act 1990 was looked at as an ideal provision to handle the issue, the matter had remained unresolved, until the UK Parliament finally passed a different law altogether, the Fraud Act 2006, to tackle the problem. However, the Fraud Act does not approach the issue from a real life technological perspective but instead creates a new perspective which does not have anything to do with the philosophy of the law of deception.[1]

The legal phobia against technology in the late 1980's circulated in other countries as well. As Hafner and Markoff (1991, p. 11) pointed out (in the United States context):

> *"...they (hackers) have mastered the machines that control modern life. This is a time of transition when young people are comfortable with a new technology that intimidates their elders. It is not surprising that parents, federal investigators, prosecutors and judges often panic when confronted with something* ***they believe is too complicated to understand****." (Emphasis added).*

The same dilemma of "the-law-is-still-not-enough" is also faced in the United States. The Federal Computer Systems Protection Act was proposed in 1977 following the Federal dissatisfaction with the "legal uncertainty" in the State approaches to computer related crimes. The main cases were *Hancock v State (1966) 402 S.W.2d 906 (Tex.Crim.App.)* and *Ward v Superior Court (1972) 3 Computer L.Serv.Rep. 206*. In *Hancock v State*, theft of computer programs was held as an offence in Texas as the programs were considered to fall under the statutory definition of "all writing ... of every description, provided such property possesses any ascertainable value". However, in *Ward v Superior Court*, theft of a competitor's computer program was not an offence where an employee manipulated his employer's computer access code to convert a program for his own benefit, since the law required the physical taking of property.

The above Federal bill failed to materialise, despite being revised and reintroduced in 1979. However, several State laws emerged, with almost half of them modelled according to the bill. The bill later re-emerged as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, and later rebranded as the Computer Fraud and Abuse Act. Specific State legislation has followed suit ever since. However, the Symantec Internet Security Threat Report (2011) ranked United States as first as far as malicious computer activities are concerned. This shows that having laws which are considered comprehensive is not necessarily a viable solution to modern cybercrimes.

3. The need for a new approach in handling modern cybercrimes

It is time to be more adaptive and responsive to technology rather than viewing it as something alien which will never match with law. When malware and badware are deployed in cybercrimes, is it a matter for the legal fraternity to suggest the same process all over again: set aside the existing cybercrime legislation and introduce brand new ones when the existing legislation can be expanded or interpreted to cater for the problem? Is it also high time to revert to the traditional legislation for the same re-expansion and reinterpretation, the cybercrime-solving-ability of which was discarded when the "distinct" cybercrime legislation was passed because of the belief back then that the traditional legislation was too old to

[1] *The Fraud Act is inter alia concerned with the concept of "false pretence". This does not represent the law of deception, but rather provides an alternative to it.*

handle cybercrimes? While the principle of *nullum crimen sine lege* prescribes that a person cannot be prosecuted unless the law formally provides that his or her behaviour is illegal despite the fact that his or her behaviour is harmful to others, the application of such a principle should not be too rigid as to deny the existing law a fair place in the realm of technology, when the law indeed has the potential to be explored for more "interpretative" possibilities.

In dealing with cybercrimes in general, there have been two schools of thought: one which separates cybercrimes from the general crimes and one which lumps cybercrimes into the general crimes category, as can be seen in the work of . While the former has the virtue of leading the legal community to a directed focus, the latter expands more flexibilities and possibilities. But whatever the approaches are, as long as the relevant provisions exist, does it really matter?

Two matters have to be distinguished here: existing legal provisions and existing enforcement methods. Brenner (2004) observed that since cybercrime is different as far as the criminal methods and the peripheral effects are concerned, it "eludes the scope of the metrics we use for crime". Therefore, current enforcement methods will never work against it since its framework, though it has evolved, is based on the model developed in the nineteenth century where proximity, scale, physical constraints and physical patterns are the key features of crimes (Brenner, 2004). That is why Wall (2007, p. 9) came to conclude that: "…more confusing is the contrast between the many hundreds of thousands of incidents that are supposedly reported each year and the relatively small number of known prosecutions."

The above point was also endorsed by Kroezynski (2008) who observed that although the United States has cybercrime legislation at both Federal and State level, this does not really assist in apprehending criminals who employ viruses and worms to cause damage to computers. Turrini (2010), after examining issues of the "deficiency in the punishment probability, lack of social stigma for committing computing crimes, and the abundance of vulnerable targets", concluded that the issues have decreased the ability of traditional deterrence mechanisms against cybercrimes and contributed towards their considerable rise. Brenner (2010) also stressed that the ability of law enforcement to act in response to cybercrimes gradually diminishes since authorities are relying on resources which are already "minimally adequate" for the physical world crimes.

The above views support the contention that there is no doubt that the current enforcement method is almost obsolete for handling modern cybercrimes. However, the existing legal provisions are still relevant, though their efficiency remains debatable. It is about determining their efficiency rather than their effectiveness. This means that there is no doubt that having proper legal provisions and proper enforcement are the right actions adopted by the legislature, but the main concern here is about bringing the actions forward in the right manner. In this connection, Kierkegaard (2008, p. 470) has remarked:

> *"The definition of cybercrime is still evolving and has now been expanded to cover any illegal act involving a computer and to all the activities done with criminal intent in cyberspace or are computer related. There is a sharp disagreement among legal experts on whether cybercrime should only include new forms of crimes that have no offline equivalent."*

Geer (2007, p. 32) pointed out that "the digital world is not the physical world" and thus "relying on intuitions derived from the physical world to make policy choices will get us into trouble every time". He stressed that "digital law is and must be counterintuitive". However, while both worlds are not the same, the only significant difference is the "space factor". Yar (2006, p. 12) observed that:

> *"It is the novel social-interactional features of the cyberspace environment (primarily the collapse of space-time barriers, many-to-many connectivity, and the anonymity and changeability of online identity) that make possible new forms and patterns of illicit activity. It is this difference from the "terrestrial world" of conventional crimes that makes cybercrime distinctive and original."*

The "space factor" refers to the physical and virtual occupation of the space by the criminals. For example, whether damage is committed offline or online, the nature of the perpetrator is still the same: human, save for the fact the cybercriminal benefits from the "space factor" to escape detection with more ease. This is due to the fact that in the virtual world people are not subject to the laws of gravity and the rules of physics, rendering the virtual but physically impossible manipulation by a person with physical disability (Brenner, 2010). Although Yar (2006) is right in his argument regarding the emergence of new forms and patterns of illicit activity, this does not necessarily lead towards a notion of distinctiveness and originality in cybercrimes. As Wiles and Reyes (2007, p. 4) point out, "cybercrime comprises the '3 Ts': tools to commit the crime, targets of the crime (victim), and material that is tangible to the crime". This means that the environment and criminal methods may be unconventional, but the criminal behaviour and impact revolve around the same thing: **damage, deception and trespass.** As pointed out by Jhankhani and Al-Nemrat (2010, p. 574):

> *"In many ways, cybercrime is no different to more traditional crime - both involve identifying targets, using surveillance and psychological profiling. The major difference is that the perpetrators of cybercrime are increasingly remote to the scene of the crime."*

4. Conclucion

The main goal for the UK and US situation is to open up possibilities by utilising existing legal provisions which have never really been properly explored. Sivasubramaniam (2010) stressed that "it is a myth that cyberspace is a lawless wilderness." He maintained that "conventional laws can and do apply to cyberspace activities". That is why the best way is to be as flexible as far as the justice system allows. The legal focus should always be on "what could be", not "what was" (Blume & Southwell, 2009). Thus virtual unjustified harms, either to persons or property or even both should be treated to a certain extent in the same manner like any other crimes. As Allan (2005, p. 178) puts it, "cybercrime ought not to become a sui generis category of offending that sits outside the established groupings of criminal conduct." The "true" nature of cybercrime is reflected in a good equation formula made by Reyes (2007, p. 9):

> *"Once an investigator removes the computer aspect of the crime out of the criminality equation (Computer + Crime = Cyber Crime) the investigator will ultimately reveal the underlying crime that has occurred (Crime = Crime)."*

What matters is to what extent modern cybercrimes fit within the established law, and if they do not fit, whether new provisions are necessary. To complement the legal provisions, a non-traditional method of enforcement is required. This is due to the fact that it is not easy to completely understand the true proportions of computer technology and its side effects while immersed in its continuing process of development (Cavelty, 2008). Of course there are already methods developed to deal with traditional viruses and worms, but the malware and badware threat is "a different kettle of fish" (Greiner, 2006).

Roman (2009, p. 487) pointed out that "computer crime statutes exist in a particular universe where misinterpretations are easy to make and hard to undo". Therefore, the proper interpretation and application of existing legislation is highly necessary to cope with the fast-paced world of ICT. Given the multifaceted nature of this breed of crime, more often than not the police and the prosecution are left with more than one legal provision to apply. In this connection, they would have to decide which is more applicable and more importantly, which best serves justice (Grabosky, 2007). As Brenner (2004, p. 5) pointed out:

> *"If online fraud is substantively undifferentiated from traditional, real-world fraud, what might justify treating it as something new, as a cybercrime? The differences that could justify treating online fraud as a distinct phenomenon - as a cybercrime instead of a crime - lie not in the elements of the offense, but rather in* ***circumstances involved in its commission.*** *" (Emphasis added).*

When it comes to applying the UK and US legislation to this breed of crime, due caution needs to be taken by those involved in the legal process to ensure that everyone has the basic knowledge of its nature. To catch a cybercriminal, it is always worthwhile to think like one. As Sun Tzu put it:

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

References

Allan, Gregor. (2005). Responding to cybercrime: A delicate blend of the orthodox and the alternative. *New Zealand Law Review*, 1, 149-178.

Bainbridge, D. J. (1989). Hacking-the unauthorised access of computer systems: The legal implications. *Modern Law Review*, 52, 236-245.

Blume, R. C., & Southwell, A. H. (2009). A sword or a shield? The new administration's approach to cybercrime and cybercrime fighting. *MAY Champion*, 33, 32-37.

Brenner, S. W. (2004). Cybercrime metrics: Old wine, new bottles? *Virginia Journal of Law & Technology*, 9(13), 1-52.

Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement? *Rutgers Computer & Techology Law Journal.*, 30, 1-114.

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. California: Praeger Publishers.

Cavelty, M. D. (2008). *Cyber-Security and threat politics: US efforts to secure the information age*. New York: Routledge.

Clough, Jonathan. (2010). *Principles of Cybercrime*. New York: Cambridge University Press.

Dumbill, E. A. (1990). Computer Misuse Act 1990 - Part 1. *New Law Journal* , 140(6467), 1117-1118.

Fafinski, Stefan. (2006). Access denied: Computer misuse in an era of technological change. *The Journal of Criminal Law*, 70, 424-442.

Garrie, D.B., & Komagome, L. R. (2008). The voyeur among us: Navigating around the global spyware epidemic. *Journal of International Technology and Information Management*, 17(2), 111.

Geer, D. E., Jr., (2007). The physics of digital law: Searching for counterintuitive analogies. In Balkin, J .M., Grimmelmann, J., Jatz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.), *Cybercrime: Digital cops in a networked environment* (pp. 13-36). New York: New York University Press.

Grabosky, Peter. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law and Social Change*, 47, 201-223.

Greiner, Lynn. (2006).The new face of malware. *networker*, 10(4), 11-13.

Hafner, Katie & Markoff, John. (1991). *Cyperpunk: Outlaws and hackers on the computer frontier*. New York: Touchstone.

Hamid Jhankhani & Ameer Al-Nemrat. (2010). Cybercrime. In Hamid Jahankhani, Watson, D.L., Me, G., & Leonhardt, F. (Eds.), *Handbook of electronic security and digital forensics* (pp. 573-584). London: World Scientific Publishing.

Kierkegaard, S. M. (2008). International Cybercrime Convention. In Janczewski, Lech & Colarik, A. M. (Eds.), *Cyber warfare and cyber terrorism* (pp. 469-476). Hershey: Information Science Reference.

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.

Lloyd , Ian. (1988). Computer abuse and the law. *Law Quarterly Review*, 104, 202.

Majid Yar. (2006). *Cybercrime and society*. London: Thousand Oaks.

Reyes, Anthony. (2007). *Cyber crime investigations: bridging the gaps between security professionals, law enforcement, and prosecutors*. Maine: Syngress Publishing.

Roman, P. V. (2009). The black box canon of statutory interpretation: Why the courts should treat technology like a black box in interpreting computer crime statutes. *John Marshall Journal of Computer & Information Law*, 26, 487-500.

Sivasubramaniam, Bahma. (2010). Watch what you say online. [Online]" Available: http:// www.thestar.com.my (September 19, 2010)

Sun Tzu & Giles, Lionel (Ed.). (2005). *The art of war*. (special ed.). El Paso: El Paso Norte Press.

Symantec Internet Security Threat Report: 2011 Trends (Volume 17, 2011).

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 Press.

Wiles, Jack & Reyes, Anthony. (2007). *The best damn cybercrime and digital forensics book period*. Maine: Syngress Publishing.