The Way Forward in Addressing Cybercrime Regulation on a Global Level

Murdoch Watney
Department of Criminal Law and Procedure
University of Johannesburg
Johannesburg, South Africa

Abstract

The proliferation of cybercrime necessitates all internet-connected states to be involved in cybercrime regulation, not only on a national and/or transnational level but also on a global level. Although it has been stated that the internet per se and cyberspace in general are by its very nature ungovernable, most nation-states have implemented national and in some instances transnational laws to regulate the internet and cyberspace for law enforcement and national security purposes. The effectiveness of such regulation in cross-border crime commission has brought about many unsolved problems which necessitate a debate on the way forward in addressing cybercrime regulation on a global level. As illustrated in the discussion, cyberspace may very well become ungovernable if a "super-power" nation-state or a cluster of nation-states take a unilateral decision regarding which conduct constitutes permissible online conduct and subsequently try to superimpose these laws on other nation-states. It is suggested that under the auspices of the United Nations and within an international law context the following issues should be addressed: conceptualizing the term "cybercrime" in establishing for example whether it includes a cyber-attack, determining which online conduct is permissible to ensure peace and security and initiating negotiations towards a cybercrime treaty. Addressing the latter issues will constitute a starting point in the way forward in ensuring cybercrime regulation on a global level.

Keywords: cybercrime regulation, global cybercrime laws, nation-state cybercrime laws, transnational cybercrime laws.

1. Introduction

In early February 2012 at a Kaspersky Lab Cyber Conference in Mexico, Michael Moran, acting assistant director of cyber security and crime at Interpol, made a call for "better laws to deal with cyber crime" [1].

His call is justifiable taking into account that cybercrime has not only evolved into what analysts call a lucrative and established "parallel economy" worth billions affecting developed and developing internet-connected countries alike, but this "shadow" industry poses a serious and growing threat to law enforcement and/or security of nation-states.

It is against this background that the call for "better laws" necessitates a discussion on the way forward in addressing cybercrime regulation. For purposes of this discussion, cybercrime regulation refers to the laws governing the prevention, detection, investigation and prosecution of cybercrime.

In establishing how "better laws" in dealing with cybercrime may be brought about, the following unresolved and somewhat controversial questions require consideration:

i. Should "new" laws be drafted, taking into account that most states have cybercrime legislation in place on a national and/or transnational level?
ii. If affirmative, who should be drafting these laws? May it be drafted by a nation-state or a cluster of nation-states on a transnational level or should it be drafted under the auspices of the United Nations within the context of the international law?
    In respect of this question, it is relevant to keep in mind that the various internet-connected nation-states represent diverse cultural, economic and political value-systems. The author of this discussion is from South Africa, a developing nation-state which in 2010 became a member state of the international political organisation of leading economies, BRICS which consists of Brazil, Russia, India, China and South Africa. It will be shown that cybercrime regulation cannot be separated from the diverse value systems that are representative of the different nation-states and that nation-states align themselves with the cybercrime regulation implemented by the different "powers."
iii. Keeping the latter observation in mind, it may be asked whether a global response for example under the auspices of the United Nations will result in so-called "better laws"?
iv. Lastly, how will compliance with the laws within the context of for example, international law, be ensured, because it may be argued that "better laws" should equal better enforcement by means of assistance and co-operation in the prevention, detection, investigation and prosecution of cybercrime.

Although it may sound dramatic, it is nevertheless not unfounded to refer to the internet and cyberspace in particular, as a battlefield of diverging and conflicting interests and opposing opinions on laws such as the protection of intellectual property rights and freedom of expression to name but a few [2][3].

What will however emerge from this discussion is that since cybercrime affects all nation-states, states have realized the importance of uniting to protect the internet and specifically cyberspace against becoming a "lawless" medium especially since the global society is dependent on information and communication technology on all levels: from e-commerce and e-governance to social networking. In this discussion the focus will be on how the different nation-states may achieve a uniform approach in the protection of the internet and cyberspace against cybercrime.

2. Defining cybercrime within the context of an electronic medium

As the discussion deals with cybercrime, the starting point should be to define the term "cybercrime." Such a conceptualisation not only serves as a point of reference to establish which conduct constitutes cybercrime, but is also relevant when determining whether the criminal investigation of cybercrime is conducted for purposes of law enforcement or national security. The latter distinction is very relevant as different agencies may be involved in the criminal investigation, the aims of the different agencies may differ and cybercrime may be dealt with differently.

Unfortunately universal definitions of cybercrime, cyber-attacks, cyber-terrorism, information warfare (iWar) and cyber-war do not exist [4]. Some definitions may be too wide and others too narrow and therefore many authors refrain from defining the term, "cybercrime" as consensus has not been reached on which conduct constitutes cybercrime.

In the absence of a universal definition for cybercrime, the concept "cybercrime" will be interpreted as an umbrella term that includes various forms or categories of unlawful conduct. Cyber-attacks have for example been included in this concept but it may be that some nation-states are of the opinion that a cyber-attack is not a cybercrime but an act of "war." The latter illustrates the relevance of drawing a clear distinction between cybercrime regulation for either law enforcement or national security purposes. Although the serious nature of cyber-attacks cannot be disputed as attacks may target critical infrastructure such as systems that run prisons and airports and utilities like power-grids and water supplies, this issue will be revisited later in the discussion as it is not clear whether a cyber-attack on a critical cyber infrastructure would constitute an act of "war" in terms of international law.

In the conceptualization of cybercrime, the differences between a crime committed in an electronic medium and a physical medium should be kept in mind as these differences impact on cybercrime prevention, detection, investigation and prosecution. Crimes were traditionally committed in a physical medium within the territory of the nation-state where a re-active approach is effective: the investigators collect the evidence – normally physical evidence - after the commission of the crime and in many instances the investigators do not need the assistance of an intermediary. The perpetrator is normally also present at the scene of the crime and/or at least within the territorial borders of the nation-state. Cybercrime may however be committed outside the borders of a country where the effect of the crime is ultimately experienced, in which case the investigators will in many instances have to rely on the assistance of an intermediary such as the service provider for the collection of evidence. This evidence will mostly be of an electronic nature and as electronic evidence is easily destroyed, a re-active approach is needed which implies that the evidence for detection and/or investigation should be collected prior to the commission of the crime. A shift from a re-active to a pro-active approach invariably impacts on individual human rights. State regulation of information by means of, for example traffic data retention, elicited human rights objections and comparisons were made to George Orwell's "big brother" (the government) watching over its citizens. As will be illustrated hereafter, cybercrime regulation faces many challenges unknown to crime regulation of the physical world: one of the big challenges relates to the balance between the protection of human rights and cybercrime prevention, detection, investigation and prosecution. There is a fine line between a police state and a surveillance state and in achieving a balance between a crime control versus a due process approach to cybercrime regulation [5].

3. Understanding cybercrime regulation of the internet and cyberspace

Cybercrime is committed within an electronic medium which evolve around the intangible, namely information within an electronic medium. Nation-state regulation of the electronic medium in addressing cybercrime for law enforcement and national security purposes can only be fully appreciated by understanding the concepts of internet and cyberspace. Cyberspace is sometimes used as an internet metaphor, a *de facto* synonym for the internet without clearly distinguishing the internet from cyberspace and confusing the two concepts.

The internet refers to the infrastructure that makes communication in cyberspace possible. As such it is an interconnected system of networks that connects computers worldwide. It relies on a physical infrastructure that connects networks to other networks using the Transmission Control Protocol (TCP) and Internet Protocol (IP). It does not comprise of a single physical entity but of an ever-growing system of networked computers that are linked to other computers. Although no one owns the internet, there are governments, organizations and institutions that own some of the computers and networks that comprise the

internet, in other words, pieces of the infrastructure. These pieces of infrastructure are located within the territorial borders of a nation-state and this part of the internet can be regulated by a nation-state.

Cyberspace denotes the "place" where communication on the internet takes place. It is "a place without physical walls or even physical dimensions – where ordinary telephone conversations 'happen,' where voice mail and email messages are stored and sent back and forth, and where computer-generated graphics are transmitted and transformed, all in the form of interactions, some real-time and some delayed among countless users, and between users and the computer itself" [6]. Cyberspace exists everywhere where there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves.

The allegation has been made that the "internet is by its nature an ungovernable environment" [1]. If one considers the evolution of nation-state cybercrime regulation of the internet from initial no-regulation to conduct regulation and ultimately to the extension of conduct regulation to include the collection of evidence, then it is clear that various states have tried to control the physical infrastructure of the internet within their jurisdictions [7]. The biggest challenge facing nation-states in cybercrime regulation is the commission of crimes outside their territory, in other words across border crimes that take place in so-called cyberspace. Cyberspace has been referred to as the fifth common space after land, air, sea and outer space and the call for "better laws" will have to address the crimes committed within the realm of this common space, the so-called cyberspace where co-ordination, co-operation and laws between different nation-states are needed [8].

4. Cybercrime regulation

As indicated, a distinction must be drawn between cybercrime regulation for the purpose of law enforcement or national security as it highlights the different challenges faced by law enforcement and national security agencies. Not only will different agencies most probably be involved but their approach and aims may differ.

4.1 Cybercrime regulation for law enforcement purposes

Most states provide on a national level for cybercrime prevention, detection, investigation and prosecution within their sovereignty. The different phases of cybercrime regulation of the internet in respect of law enforcement illustrates that state cybercrime laws should encompass more than merely criminalizing unlawful conduct but also deal with procedures in the prevention, detection and investigation of crime and collection of evidence for subsequent prosecution.

Although a state may have cybercrime laws on a national level in place, it does not automatically imply that it is being enforced. The non-enforcement of these laws results in what may be referred to as so-called "paper laws." Many reasons are advanced for non-enforcement, one being that the law enforcement entities of some countries lack the technical expertise as well as the financial means to have sufficient technical security in place. The latter may be true especially in respect of some developing countries [4]. The issue of enforcement of laws will be discussed hereafter and more specifically in relation to the application of extra-territorial jurisdiction.

Many commentators have alluded to the challenges facing across border cybercrime commission and investigations [4]. Across border crime commission (also referred to as multi-jurisdictional crime) affects many jurisdictions and in respect of law enforcement co-operation, issues such as sovereignty and dual criminality to name but a few, may become stumbling blocks. Cloud computing serves as an example in this regard: where the data in the "clouds" is data that is constantly being shifted form one server to the next, moving within or between different countries at any time, resulting in jurisdictional challenges [8]. As a result there is an urgent need for harmonization of laws in respect of cybercrime prevention, detection, investigation and prosecution. This ultimately results in the question as to which body will ensure such harmonization of cybercrime laws. The only treaty at present that may be used as a guideline for such harmonization of laws is the Council of Europe (CoE) Convention of Cybercrime (Cybercrime Convention) of 2001. Although the issue of harmonization will be discussed hereafter, it is important to note that harmonization has not yet been affected.

Unlike physical crime, cybercrime may be committed from a country's territory without the physical presence of the accused. It is acknowledged that many forms of cybercrime such as child pornography, advance fee payment fraud and money laundering cannot be dealt with by national laws alone and in addressing cross-border or multi-jurisdictional crimes co-operation and assistance by means of transnational laws are required. However, in many instances there will not be co-operation and assistance on a transnational level and this will jeopardize the investigation and ultimate prosecution of the perpetrator. As a result perpetrators are not apprehended which are detrimental to crime control management. The much coined quote "justice is only done if it is seen to be done" is very relevant in respect of prosecution. Unfortunately, even where the accused is identified, a request for his extradition from the country where the crime originates and most probably the country of which the accused is a citizen and the country where the effect of the crime is felt, may be contentious and have diplomatic repercussions [7]. The latter is illustrated with reference to the extradition request in 2005 by the United States of America (US) to the United Kingdom (UK) for the extradition of a UK citizen, McKinnon, who allegedly hacked from the UK into 97 US military, navy and NASA computers between February 2001 and March 2002. Although the US has requested the extradition of McKinnon

in terms of objective territoriality, he has not as yet been extradited due to various legal objections from the UK. The latter may be avoided by applying the international law and considering the application of subjective and objective territoriality in respect of cybercrime. In terms of subjective territoriality the country of origin may prosecute the accused citizen whereas in terms of objective territoriality the country where the effect was felt may insist on prosecution. Similarly a South African citizen, Roach, sent e-mails and letters to the UK and the US in 2010 and early 2011, threatening to launch a biological warfare if a certain amount of money was not paid over to him. South Africa established subjective territoriality and the accused was prosecuted and sentenced in 2011.

4.2 Cybercrime regulation for national security purposes

Cybercrime regulation for the purpose of national security refers to crimes that may affect the critical infrastructure of a nation-state. Critical infrastructure may be defined as all services that are fundamental to the effective operation of a nation state such as its transport system and economical system. Most nation-states have already or are in the process of, drafting national cyber security policies or legislation. Although many of the challenges referred to in relation to cybercrime regulation for law enforcement purposes are also experienced in respect of cybercrime regulation regarding national security purposes, cybercrime committed against the critical infrastructure will most probably not only have diplomatic repercussions, but as indicated hereafter, there are also issues inherent in the cybercrime regulation for national security that are not part of the law enforcement of cybercrime.

A nation-state should be in a position to protect its critical infrastructure as a government has an obligation to protect its citizens against harm or injury. It is however an open question on how far a country may go in developing the technical means of protecting its infrastructure. Most countries have the technical means in place to defend its critical infrastructure. In 2011 the US Congress authorized the US military to conduct offensive military activities in cyberspace [9]. However, in August 2012 the US Senate rejected the Cyber Security Act of 2102 aimed to protect the US from cyber attacks. Various objections were leveled against the act *inter alia* in respect of its human rights implications (infringing of privacy rights) and that the powers it gave the Department of Homeland Security to determine what is understood with "critical infrastructure," were too wide [10]. Regarding the protection of a state's critical infrastructure, a multi-faceted approach has to be applied: co-operation is required between companies, institutions, private citizens and government departments but once again the issue that presents itself is how invasive this co-operation might be before the power to collect evidence of a possible attack borders on that of a "police" state [11].

Although a nation-state should have policies in place for protecting its critical information infrastructure, in many instances the threat will originate from outside its borders. The latter is illustrated by the much publicized cyber-attack launched against the nation-state, Estonia. On approximately 27 April 2007 Estonia was hit by a blizzard of DDoS attacks launched against important Estonian websites, such as those of the president, parliament, leading ministries, political parties, major news outlets and Estonia's two dominant banks [12]. The attacks brought the internet in Estonia to a grinding halt and the country was severely affected, more so than a country less dependent on the internet. In order to ascertain the type of cyber-attack launched, it is relevant to establish the method used in the attack, the motive as well as the target of the attack. The DDoS attacks were presumably launched in protest against Estonian officials for moving a bronze statue of a Soviet soldier from a park in Tallinn, Estonia's capital, to a military cemetery. Ethnic Russians, which makes up about a quarter of Estonia's population, as well as Russia regarded this as an affront to the memory of soldiers who fought the Nazis during World War 2. In contrast most Estonians felt that the statue represented a symbol of almost five decades of Soviet occupation which ended when Estonia became independent from the Soviet Union in 1991.

The attacks on Estonia illustrated the following to all internet-connected countries: it is not always easy to establish with certainty what type of cyber-attack was launched, namely whether the attack constitutes cyber-terrorism or i-War or cyber-war. Although a fine line exists between investigating crime in the interest of law enforcement and that of national security and most crimes will clearly fall either within the domain of law enforcement or national security, it is not always so easy to establish this in respect of cyber-attacks. It was for example alleged that the Estonia incident was cyber-warfare as the nation-state Russia was involved, although Russia denied this allegation [13]. Others were of the opinion that it was an orchestrated protest attack by a group of disgruntled Estonian citizens of Russian descent, an example of i-War [12]. Some commentators referred to the attack as cyber-terrorism [14]. The opinion was also expressed that the attack on Estonia was not cyber-warfare as it was not accompanied by a military offensive in the real world which was the case in respect of the cyber-attacks on Georgia in 2008 [15]. Blaming so-called culprit nations for instances of cyber-attacks with the aim of espionage serves no purpose if these allegations are not substantiated by supporting evidence. Mere allegations result in diplomatic and political conflict which does not assist in addressing cybercrime.

The Estonian attack illustrated that all countries are vulnerable to attack and this gives credence to the fact that a cyber-attack is an international issue. Internet-connected countries have come to realize that although the internet has

many advantages, the negative side thereto was reflected in Estonia.

Unfortunately - as already indicated and which will be alluded to again - the protection of cyberspace cannot be negotiated between nation-states on a transnational and diplomatic level. This may be frustrating to nation-states as reflected in the deadlocked talks of 2009 between Russia, the US and a United Nations arms control committee aimed at strengthening cyber-security and limiting the military use of cyberspace [16]. Some nation-states may be of the opinion that another nation-state is trying to generally super-impose its own laws and that it is advancing only its own interests.

On an international level questions such as which type of attack constitute cyber-war and whether a victim state may launch a counter-attack on the alleged perpetrator will have to be revisited. In terms of article 51 of the United Nations Charter a nation-state has the right to self defense but only if the state was attacked with armed force. May a cyber-attack such as that launched against Estonia in 2007 be termed as "armed force"? It is debatable whether a country may retaliate in terms of article 51 but it is surely an issue that should be re-visited within the international law context and also against the background of a changing globalized world.

4.3 Conclusion regarding national and transnational cybercrime regulation

It is not so much a question of what is "wrong" with a nation-state's cybercrime laws on national and transnational level, but rather whether it is effective within an electronic and global medium such as the internet and in general cyberspace.

As illustrated, the problem presents itself with cross-border crimes as assistance and co-operation from other nation-states may be needed. Some of the states required to assist may be unwilling or not in the position to give assistance. The latter issue should be addressed on a global level.

Despite the existence of nation-state laws on national and transnational level the internet and cyberspace may become ungovernable if unilateral decisions, despite being well intended, are taken for example in respect of which conduct constitute permissible conduct in cyberspace.

Law enforcement and national security within an electronic medium and specifically a global medium that is accessible to all nation-states, face challenges that are dissimilar to that experienced within a physical medium. This medium necessitates "new" laws on a global level which will address the following issues:

- Ensure all states have cybercrime laws in place on national and transnational levels;
- Harmonise a state's cybercrime laws specifically pertaining to multi-jurisdictional crimes;
- Conceptualize the legal position regarding certain forms of cybercrime such as the launch of a cyber-attack from one state against another; and
- Address enforcement of these laws.

5. Moving towards global cybercrime regulation

Calls for a global multilateral treaty dealing with cybercrime have intensified since 2010. It has become clear that an international response is needed, specifically in respect of transnational cybercrime.

In 2011 Russia, China, Tajikistan and Uzbekistan sent a letter to the UN Secretary General Ban Ki-moon calling for a UN resolution on a code of conduct relating to the use of information technology by countries [17]. The proposed UN resolution calls for countries to co-operate in order to combat criminal and terrorist activities involving cyberspace. It also calls on countries to undertake not to use technology to carry out hostile acts of aggression. The code provides that a nation-state should be in a position to protect their "information space" and critical information infrastructure from threats, disturbance, attack and sabotage.

As already indicated, state cybercrime laws are not harmonized. The question that invariably comes to mind is whether the Cybercrime Convention could be used as an instrument for harmonization. What should be considered in this regard is that although the Cybercrime Convention came into operation in 2004 and is a laudable instrument as such, it is not an international treaty as some commentators have indicated [18]. The majority of the CoE member countries and four non-European member countries namely the US, Japan, South Africa and Canada became signatories. Russia, also a CoE member, refused to become a signatory as it is of the opinion that article 32 of the Convention infringes sovereignty since it provides for cross-border access to information [19].

There has been a suggestion based on viable arguments that the Cybercrime Convention could be used as a framework for drafting a UN treaty [18]. In 2009 Schjolberg and Ghernaouti-Hellie presented a proposal for a *Global Protocol on Cybersecurity and Cybercrime* which, according to Gercke, is based on the wording of the provisions provided by the Cybercrime Convention [3]. It unfortunately appears, whether justified or not, that the main argument against the Cybercrime Convention relates to the perception that it is a predominantly European instrument. Another point of criticism against the Cybercrime Convention is that it is outdated as it was drafted without due consideration to terrorism [18]. Without elaborating in detail on the criticism, it appears that the Cybercrime Convention is not an instrument that would unite all internet-connected countries, nor could it be used as a framework to direct discussion.

As already alluded to, cybercrime regulation cannot be separated from global politics. All states will not automatically follow the guidance of a superpower nation-state. This has been illustrated by Russia's refusal to sign the Cybercrime Convention and its rejection of a draft of the *Declaration on Fundamental Freedoms in the Digital Age*

presented by the US secretary of state at the Organisation of Security and Co-operation in Europe Summit (OSCE) in 2011 [20]. Russia has also been vocal in calls for a UN cybercrime treaty [21].

Although South Africa for example signed the Cybercrime Convention in 2001, it is unlikely that South Africa will ratify it. It should be added that South Africa did implement legislation that comply with the framework of the Cybercrime Convention. South Africa's alignment to BRICS will in all probability prevent its ratification of the Convention.

What should be considered at this stage in the absence of a global cybercrime treaty, is a UN resolution outlining which conduct is permissible in cyberspace to ensure peace and security [17]. This will be a step in the right direction albeit a preliminary one.

A UN resolution on conduct in cyberspace does not imply that negotiations on a UN Cybercrime Convention should not commence. Many have expressed reservations regarding the success of such negotiations and although it will not be an easy task, these negotiations will benefit the global internet community [18]. The fact that nation-states are suggesting a code on permissible cyberspace conduct may serve as an indicator of the willingness of nations-states to discuss internet regulation.

6. United Nations intervention equals "better" laws

This brings one to the following question: Will global intervention bring about "better" laws? As a point of departure the concept "better" laws requires elucidation.

Relevant is the already discussed proposed code of conduct which will bring states together under the auspices of the United Nations and on the basis of voluntary participation. Although the code may be seen as so-called "soft law" which is not binding on states it does carry some authority. As already indicated, some nation-states may hold the view that cybercrime laws initiated by individual states or cluster states may not be transparent or that a (certain) nation-state(s) is vying for dominance in respect of the internet. A code of conduct will not necessarily bring about better "laws", but will identity the rights and responsibilities of all nation-states in respect of the "information" space and may result in a more co-ordinated effort to make the internet safer, especially in respect of cyber-attacks and terrorist activities.

How can "better" laws regarding cybercrime be implemented? It can only be done by means of a UN treaty on cybercrime. This treaty will not replace the nation-states' national and transnational cybercrime laws but will supplement the nation-states' regulation, give nation-states the opportunity to align their laws thereto and go a long way in the harmonization of nation-states' laws to ensure cross-border investigation and prosecution.

7. Enforcement of cybercrime laws

Effective enforcement of cybercrime laws can only be achieved in terms of a UN treaty within the ambit of international law. All states must take responsibility to enforce cybercrime regulation. If need be, there should be assistance by other nation-states, especially to states such as developing states that does not have the technical and/or financial means to enforce these laws.

Schjolberg who is a strong supporter of an international criminal court for the most serious of cybercrime in cyberspace makes a valid point when he remarks that the most serious cyber-attacks have so far not resulted in investigation and consequently prosecution and that an international criminal court for cyberspace should address this void [8]. Schjolberg refers to a statement made by the prosecutor, Ferencz at the Nuremberg War Crimes Tribunal that stated: "There can be no justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under the given circumstances" [8]. Although there is merit in the call for an international criminal court, such court cannot be established in the absence of a global cybercrime treaty and therefore a discussion of an international criminal court or tribunal for cyberspace remains academic.

In the meantime, in the absence of an international court, it is suggested that nation-states make provision for extra-territorial jurisdiction in respect of serious cybercrime. Extra-territorial jurisdiction is not the same as universal jurisdiction but will provide for the position where a perpetrator committed the cybercrime outside the territory of a nation-state and he is within the territory of the nation-state or a national of that state, then the nation-state will have jurisdiction to prosecute the perpetrator for the crime. This will address the problem of a nation-state not instituting prosecution. A practical obstacle in this regard may be the lack of evidence and the challenge to obtain co-operation. However, the latter may be addressed by the proposed UN code of conduct and then ultimately a global treaty on cybercrime.

8. Conclusion

What should be the way forward for cybercrime regulation? It is clear that the internet and specifically cyberspace do not belong to a specific nation-state nor a cluster of nation-states but to all nation-states. Although nation-states realize that cybercrime and cyber-attacks affect all of them, the question of how regulation should be addressed, is a contentious issue. If a nation-state attempts to super-impose its laws on other states or take unilateral decisions, other states may retaliate with the consequence that a valuable opportunity will be lost: an opportunity for a global agreement on which conduct is permissible in cyberspace and a global cybercrime treaty. It appears that many nation-states favor regulation under the auspices of the United Nations. The latter will promote transparency and ensure that all states are involved in the negotiations.

Cyberspace ultimately belongs to the global world and despite the different – and in some instances opposing – views, all nation-states should be in agreement that cybercrime, cyber-attacks and terrorist activities may end the economic and social advantages cyberspace holds for generations to come.

9. References

[1] *Sunday Times Business Times*, 12 Feb 2012, p. 10.
[2] Kirk, J. (2012) 'Russia pushes for online conduct at United Nations General Assembly'; http://www.computerworlduk.com/news/public-sector/33079 (16 February 2012).
[3] 'Information Policy: Cyberspace: battle for 7th Continent'; http://www.i-policy.org/ (09 February 2012).
[4] Gercke, M. 'Understanding cybercrime: a guide for developing countries'; http://www.itu.int/dms_pub/itu-d/oth/01/OB (23 February 2012).
[5] Watney, M.M. in Jahankhani, H. *et al* (2010) Handbook of Electronic Security and Digital Forensics, p. 549, World Scientific Publishing Co, London.
[6] Tribe, L.H. 'The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier'; http://www.fiu.edu/~mizrachs/CyberConst.html (22 March 2008).
[7] Watney, M. M. 'A South African Perspective on Mutual Legal Assistance and Extradition in a Globalized World', 2012 Potchefstroom Electronic Law Journal (PELJ), pp. 292-318.
[8] Schjolberg, S. 'An International Criminal Court or Tribunal for Cyberspace (ICTC)' p. 3, Paper for the EastWest Institute (EWI) Cybercrime Legal Working Group; http://www.cybercrimelaw.net/documents/International_Criminal_Court_Tribunal_for_Cyberspace_(ICTC).pdf (22 February 2012).
[9] Aftergood, S. 'Congress authorizes offensive military action in cyberspace'; http://www.fas.org/blog/secrecy/2011/12/offensive_cyber.html (21 February 2012).
[10] http://www.digitaltrends.com/web/senate-votes-against-cybersecurity-act-of-2012 (2 August 2012).
[11]http://www.guardian.co.uk/commentisfree/2012/aug/02/cybersecurity-act-surveillance... (4 September 2012).
[12] Ryan, J. 'Outbreak of iWar imminent' 2008 Commercial Crime Journal, pp. 10-11.
[13] Jones, W. 'Estonia calls for EU law to ban cyber attacks'; http://www.crime-research.org/news/12/03.2008/3248/ (19 March 2008).
[14] Heath, N. 'NATO: Cyber terrorism as dangerous as missile attack'; http://www.crime-research.org/news/10.3.2008/3241/ (19 March 2008).
[15] Kirchner, S. 'Distributed Denial-of-Service Attacks Under Public International Law: State Responsibility in Cyberwar' 2009 ICFAI University Journal of Cyber Law, pp. 10-23.
[16] Strydom, H. 'Some (perhaps unforeseen) international law and relations in the time of globalization' 2009 Discourse, University of Johannesburg, p. 34.
[17] United Nations General Assembly, '66th Session Developments in the field of information and telecommunications in the context of international security'; http://www.chinadaily.com.cn/cndy/201109/14/content_13680896.htm (09 February 2012).
[18] Harley, B 'A global convention on cybercrime?' 2010 Columbia Science and Technology Law Review; http://www.stlr.org (20 February 2012).
[19] Computer Crime Research Center, 'Putin defies convention on cybercrime'; http://www.crime-research.org/news/28.03.2008/3277, (20 February 2012).
[20] 'Moscow blocks OSCE declaration on freedom of internet and starts limiting access to KC'; http://www.kavkazcenter.com/eng/content/2011/12/07/15473 (09 February 2012).
[21] Isakova, Y. 'Russia opts for universal anti-cybercrime convention'; http://englsih.ruvr.ru/2011/07/20/53481702.html (21 February 2012).

