12-3-2012

Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework

Krishna Prasad
Edith Cowan University

DOI: 10.4225/75/57a2d38a8af77
3rd Australian Counter Terrorism Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

CYBERTERRORISM: ADDRESSING THE CHALLENGES FOR ESTABLISHING AN INTERNATIONAL LEGAL FRAMEWORK

Krishna Prasad
Edith Cowan University, Western Australia
Perth, Western Australia
k.prasad@ecu.edu.au

Abstract

The increase of international cyberterrorism in recent years has resulted in computer-based criminal activities that generate worldwide fear, destruction and disruption. National laws and policies that address cyberterrorism are mainly limited to developed nations and are not cohesive in managing 21st century cyberterrorism. Given the absence of an international legal framework to address cyberterrorism, authorities and governments around the world face extreme challenges in finding and prosecuting those responsible for cyberterrorism. This article argues for the need for a cohesive international legal framework; highlights key elements to establish an effective international legal framework; and identifies existing international treaties and cross-border agreements that could be expanded to provide legislative guidelines for prosecution.

Keywords
Cyberterrorism, international legal framework, definitions, challenges, United Nations, international treaties, jurisdiction, prosecution.

INTRODUCTION

In recent years there has been growing concern about cyberterrorism and the need to implement legislation and enforcement measures to address and prosecute perpetrators in planning and organising a terrorist attack. In terms of logistics, any number of perpetrators can plan and execute attacks regardless of where they are located around the world, from sources including individuals, organised crime syndicates and agencies. Some cyber terror attacks have been carried out by organizations sponsored by other nations (Robinson, 2012). The attacks can target any facility that uses a computer network. The growing number of cyber terrorist activities highlights the difficulty nation states are experiencing in terms of locating and prosecuting perpetrators of cyberterrorism in the digital age.

It is promising to see increasing international focus being given to the issue of emerging threats in cyber security and the need for a legal framework (incorporating international treaties and agreements) to develop measures for jurisdictional prosecution and cross-border enforcement (International Atomic Energy Agency, 2011). However, while the international community has created a broad set of guidelines, existing international conventions and legislation either do not incorporate cyberterrorism or are not far-reaching enough to be effective. The lack of a cohesive international legal framework has resulted in some individual nation states proactively developing, implementing and enforcing their own domestic laws to address cyberterrorism. Considerable international cooperation and collaboration is required to develop and establish an international legal framework to provide nation states with effective legal measures to locate and prosecute perpetrators of cyberterrorism.

THE NEED FOR AN INTERNATIONAL LEGAL FRAMEWORK

Cyber terrorists target systems that are predominantly operated and controlled by computers. These systems could include critical infrastructure such as utilities (water, electricity and gas supplies), air-traffic control systems, banking and finance, telecommunications and transport systems (Grabosky and Stohl, 2003). Cyberterrorism presents extreme risks and danger for critical infrastructure (Australian Crime Commission, 2011). In Australia, governments (both commonwealth and state) define critical infrastructure as:

> Those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security. (Attorney-General's Department, 2010)

Cyberterrorism also poses real threats to the loss of human lives (Mele, 2010). In 2010, the Stuxnet worm virus that targeted the Iranian nuclear program (Fildes, 2010) could have had potentially dangerous consequences for the population, neighbouring states and other countries worldwide. Studies show that the Stuxnet virus also impacted computer networks controlling utilities in distant countries including United States, Indonesia, India, Azerbaijan, Pakistan, etc. (Symantec, 2010). Thus governments have to give considerable attention to its critical infrastructure including military and nuclear installations from being the subject of a cyber terrorist attack.

The ability of governments to prevent and deal with such attacks is dependent on a number of factors, the most important being the existence and implementation of appropriate legislation. Given the current lack of international regulation on cyber terrorist attacks, the onus is on individual countries to rely on their domestic laws to take legal action. Prosecuting the perpetrators' for such attacks is successful where the perpetrator resides in the same country. In Australia, a former council employee was jailed for two years in 2001 for hacking into council computers controlling critical infrastructure and programming them to pump millions of litres of raw sewage into public waterways (*R v Boden* [2002] QCA 164). If authorities identify that the attacker is situated in another country, the cooperation and reciprocation of that nation is necessary and may not always be forthcoming. In such instances, reliance on international organizations and other nations will be required to prevent the attack and to also prosecute the person(s) responsible for the attack. In 2007, a spate of massive cyber attacks in Estonia on the country's largest banks, newspapers, schools and many other institutions resulted in the urgent request from Estonia for a 'firm EU, NATO response to the new form of warfare' (SMH, 2007; Appathurai, 2007).

The complexity or sometimes incapacity to prosecute cyber terrorists operating in jurisdictions outside of the country of attack highlights problems concerning the lack of an international framework. Added to this is the fact that legal procedures and systems vary from country to country and the international courts actually have very limited powers making enforcement difficult. This supports the argument for the expansion of the current limited applicability of international laws on cyber terrorism and the need for an effective international legal framework.

ESTABLISHING AN EFFECTIVE INTERNATIONAL LEGAL FRAMEWORK

The four key critical elements for establishing an effective international legal framework are: agreement on the definition of cyberterrorism; leadership by the United Nations (UN); utilization and expansion of existing international conventions, legislation and authorities to create a cohesive and robust system; and effective law enforcement.

Definitions of cyberterrorism

The first critical element of an international legal framework to counter cyberterrorism is for the international agreement and acceptance of a set of definitions of terminology relating to cyberterrorism. To date the UN has developed fourteen Conventions and four amendments against international terrorism which relate to specific terrorist activities (United Nations, n.d.). However within these Conventions, there still remains no universally accepted definition of what terrorism actually is. Instead, Member States are asked to refer to the Conventions in their totality and develop their own definitions.

The international community has begun addressing this issue with the creation of the United Nations Counter-Terrorism Committee Executive Directorate (CTED) in 2010. The role of the CTED is to 'look at national legislation and if it found the definition [of terrorism] too wide, it would bring that to the attention of the country' (Smith, 2010). Nevertheless, this lack of clarity on the definition of cyberterrorism has been acknowledged as a major issue by many countries, with many (including Australia) developing their own legislation to address this issue on a domestic level.

In Australia, the *Security Legislation Amendment (Terrorism) Act 2002* (Cth) introduced into the *Criminal Code Act 1995* (Cth) the definition of a 'terrorist act' in 2002. The *Criminal Code Act* (s. 100.1(1)) describes a 'terrorist act' as 'an action or threat of action where:

(a) .....

(b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and

(c) the action is done or the threat is made with the intention of:

(i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or

(ii) intimidating the public or a section of the public. '

The *Criminal Code Act* (s. 100.1(2)) further states that an action will fall within the definition of a 'terrorist act' if it:

(a) causes serious harm that is physical harm to a person; or

(b) causes serious damage to property; or

(c) causes a person's death; or

(d) endangers a person's life, other than the life of the person taking the action; or

(e) creates a serious risk to the health or safety of the public or a section of the public; or

(f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:

(i) an information system; or

(ii) a telecommunications system; or

(iii) a financial system; or

(iv) a system used for the delivery of essential government services; or

(v) a system used for, or by, an essential public utility; or

(vi) a system used for, or by, a transport system.'

Although this definition has been adopted in Australia, other countries or organizations have different definitions. For example, Article 1 (2) of the Organization of the Islamic Conference Convention on Combating International Terrorism defines terrorism as:

> Any act of violence or threat thereof notwithstanding its motives or intentions perpetrated to carry out an individual or collective criminal plan with the aim of terrorizing people or threatening to harm them or imperiling their lives, honor, freedoms, security or rights or exposing the environment or any facility or public or private property to hazards or occupying or seizing them, or endangering a national resource, or international facilities, or threatening the stability, territorial integrity, political unity or sovereignty of independent States. (OIC, 1999)

However Article 2 (a) of the Convention states that 'Peoples struggle including armed struggle against foreign occupation, aggression, colonialism, and hegemony, aimed at liberation and self-determination in accordance with the principles of international law shall not be considered a terrorist crime'. For instance, if perpetrators of a cyber terrorist act on Australia are located in Afghanistan (one of the 57 member states to the Convention) they could claim that their terrorist act was an act of struggle against foreign occupation and hence does not fall under the definition of a terrorist crime.

Leadership by United Nations

The UN must be the catalyst for change and act as a facilitator for member states to convene and gain agreement and common understanding of cyberterrorism. Agencies within the UN like the International Atomic Energy Agency is currently working with its member states with the goal of creating an appropriate international legal framework for prosecuting cyber security events (International Atomic Energy Agency, 2011).

The UN could utilise the CTED in playing a major role in harmonising the variety of domestic criminal laws to manage offences in the area of cyberterrorism by facilitating member states with opportunities of discussing broader critical issues of information sharing and jurisdictional prosecution measures on terrorists. Since 2010, the CTED have 'carried out a dialogue with all 192 Member States on what measures they had taken to criminalize terrorism, bring terrorists to justice, prevent financial support to terrorists, and prevent them from getting safe haven and crossing borders' (Smith, 2010). One can argue that expanding the powers and mandate of the CTED beyond its current role, could lead to a unified legislative framework which includes standardised key terms of references for Member States.

The UN is the ideal forum where agreement could be obtained on ensuring the domestic laws of all member states (including developing countries) provide adequate powers for cyberterrorism investigation and prosecution. This international collaboration could proactively work towards establishing a swift, responsive and effective coordination management system for cyber intelligence sharing. Joint agreement could also be reached on guidelines to ensure comprehensive responses to cyber attacks that are appropriate, proportionate and cost-effective.

Conventions, legislation and authorities

Existing conventions and treaties that hav**e** been (and continue to be) ratified by countries provide a strong foundation upon which international collaboration can be based. Although they provide a broad set of guidelines, they need to either incorporate cyberterrorism or need to be expanded (legislatively and regionally) to be effective to address and counter global cyberterrorism.

To create an effective international legal framework, existing treaties and conventions must be expanded to include comprehensive guidelines that allow for the development of domestic legislation against cyberterrorism. These guidelines must also incorporate and allow for mutual collection and sharing of information so that enforcement agencies can utilise international resources to combat perpetrators.

Convention on Cybercrime of the Council of Europe

The Convention on Cybercrime of the Council of Europe is the only binding international instrument on cybercrime (Council of Europe, n.d.). The Convention provides a general framework for developing comprehensive national legislation against cybercrime as well as international cooperation between State Parties to this treaty. In order to make this Convention more effective, it needs to expand beyond its current relevance and application to Europe. Another major factor is that the Convention only addresses 'crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security' (Convention on Cybercrime, n.d.) and does not specifically include cyberterrorism. To be an effective mechanism, cyberterrorism must be included.

This Convention has potential for development as at September 2012, 37 countries including the USA, Japan, Canada and South Africa have ratified the Convention. The ten countries that are yet to ratify the Convention hinder the Convention's effectiveness as a mechanism to develop and introduce similarity between domestic laws and investigations to combat cyberterrorism. This in turn impacts on efforts to gain commitment from the international community to criminalise cyber terrorist attacks. Despite this, over 100 nations are strengthening their domestic legislation by using the Convention as the basis to combat the threat of cybercrime (Attorney General of Australia, 2012).

North Atlantic Treaty Organization

The North Atlantic Treaty Organization's (NATO) tangible commitment to tackling cyberterrorism is the creation of the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence. NATO is now creating a Rapid Reaction Team to fight a cyber attack and is expected to be operational by the end of 2012 (NATO, 2012).

Australia

Australia's commitment to developing cyberterrorism legislation began in 2001 when the Australian Federal Government amended the *Criminal Code Act* to sanction the *Cybercrime Act 2001* (Cth) to encompass new 'Computer Offences' with serious penalties such as life imprisonment for unauthorised access, modification or impairment of data held in a computer with intent to commit a serious offence (s 477.1). This legislation also places an obligation on businesses to implement valid compliance systems for unauthorised access as well as check and identify breaches of access. These measures prevent unauthorised users accessing the system as well as limit authorised users to certain files. In Australia, cybercrime offenders have been successfully prosecuted since 1990 such as *R v Belkin* noted in Compulaw Review, (1990) 28 (6) LSJ (cited in Latimer, 2012. p.99) and *R v Boden*.

In 2002, the Australian Federal Government introduced laws to protect Australia from both terrorist attacks and from crimes of online and computer terrorism which included:

- *Security Legislation Amendment (Terrorism) Act 2002* (Cth);
- *Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002* (Cth);
- *Suppression of the Financing of Terrorism Act 2002* (Cth); and
- *Telecommunication Interception Legislation Amendment Act 2002* (Cth).

The role of the National Security Adviser also reinforces Australia's efforts to combat cyber terrorism with a specific role of:

- Developing effective partnerships within the national security community;
- Improving the national security community's strategic direction;
- Supporting whole-of-government security policy development and crisis response;
- Overseeing the implementation of all national security policy arrangements; and
- Promoting a cohesive national security culture.

(Department of the Prime Minister and Cabinet, 2012)

Australian Security Intelligence Organization (ASIO) responded to the increased global threat of cyberterrorism by creating a new Cyber Espionage Branch in July 2010 to investigate and provide advice on state-sponsored cyber-attack against Australia's interests. By June 2011, ASIO received authorisation from the Attorney-General 'to liaise with 334 authorities in 123 countries' to engage with other countries in efforts to address matters including:

- counter-terrorism;
- counter-espionage;
- cyber-threats; and
- counter-proliferation;

(Australian Security Intelligence Organization [ASIO], n.d.)

In September 2011, the Former Minister for Foreign Affairs (2011) called for public discussion and feedback regarding the importance of cyberspace to Australia's social well-being, economic prosperity and broader national interests. In August 2012, the Cybercrime Legislation Amendment Bill 2011 (Cth) passed the

Australian Senate allowing the country to become party to the Council of Europe Convention on Cybercrime (Attorney General for Australia, 2012).

Overall, the raft of Australian legislation together with criminal law cases supports the fact that the Australian legal system is competent of prosecuting offences including cyber terrorist acts committed by the use of computers. However, a concern is that this legislation is only effective provided the perpetrator is in Australia or an Australian citizen overseas. If the cyberterrorism act was carried out by a person (who is not an Australian citizen) in a country that has no extradition treaty with Australia, then that person cannot be prosecuted in Australia or in an international court without an international legislation and framework. If the country in which the perpetrator resides has weak laws or varied definitions on cyberterrorism, then no prosecution is possible in that country either.

Effective Law Enforcement

There remain many challenges for law enforcement agencies in relation to cyber terrorism. The rapid advancement of computer technology has increased the frequency and impact of cyberterrorism worldwide. These cyber terrorists continue to operate in a borderless environment with the knowledge that there is no single international legislation. Governments have varying technical competencies to deal with cyber terrorist acts and the coordination among law enforcement authorities are restricted by foreign policies and political ideologies. Law enforcement agencies around the world are also limited by resources in relation to funding and personnel trained in cyberterrorism. This in turn raises the issue of developing a secure mechanism for transferring and sharing information on cyber threat data to law enforcement agencies. One could argue that the current international legislative environment provides very limited or no deterrence for perpetrators committing cyberterrorism.

In order for countries to counter cyber terrorism, it is critical for governments, their respective law enforcement agencies and industry to stop working in silos. Coordinated international action is the only way to tackle this global issue which is affecting countries on an increasingly greater scale. A cultural shift needs to occur among all governments, information technology, law enforcement and legal sectors. Law enforcement agencies and industry need to cooperate to improve the sharing of information – particularly their swiftness in identifying and alerting new and emerging threats, including modes of attack. A comprehensive education and awareness program for lawyers, judiciary and the public on cyberterrorism could also contribute to a higher likelihood of cyberterrorism prosecution. Industry and enforcement agencies must also increase and improve their understanding of the legal process and requirements for evidence collection and presentation in judicial process. This will facilitate more accurate systemised investigations and will lead to more reliable information being brought before courts.

CONCLUSION

It is evident that existing international conventions and treaties are not effective in prosecuting and combating cyberterrorism. Thus a cohesive international legal framework is required to meet the challenges posed by cyberterrorism. To create an effective framework, existing treaties and conventions must be expanded to include comprehensive guidelines regarding cyberterrorism. These guidelines must also incorporate and allow for mutual collection and sharing of information by enforcement agencies.

Any delay in establishing an international legal framework to address cyberterrorism will send a clear message to cyber terrorists that governments and international agencies have limited or no capacity to legally pursue them. Even after an international legal framework is established, the main challenges will lie in policing and detection of such crimes by law enforcement authorities.

REFERENCES

Appathurai, J. (2007). North Atlantic Treaty Organization [Press Briefing], Retrieved from http://www.nato.int/cps/en/natolive/opinions_8313.htm?selectedLocale=en accessed on 30 September 2012

Attorney-General's Department. (2010). *Critical infrastructure resilience strategy*. Canberra: Commonwealth of Australia.

Attorney General for Australia 2012 - *New laws in the fight against cyber crime*, 22 August 2012. Retrieved from http://www.attorneygeneral.gov.au/Media-releases/Pages/2012/Third%20Quarter/22August2012-Newlawsinthefightagainstcybercrime.aspx accessed on 30 September 2012

Australian Crime Commission, (2011). *cyber crime*. Retrieved from http://www.crimecommission.gov.au/publications/crime-profile-series-fact-sheet/cyber-crime accessed on 30 September 2012

Australian Security Intelligence Organization [ASIO]. (n.d.). *ASIO Report to Parliament 2010–11*. Retrieved from http://www.asio.gov.au/img/files/Part-2.pdf accessed on 30 September 2012

Convention on Cybercrime, n.d – Summary. Retrieved from http://conventions.coe.int/Treaty/en/Summaries/Html/185.htmCouncil of Europe, n.d. accessed on 30 September 2012

Council of Europe, n.d., Retrieved from http://www.coe.int/t/dghl/standardsetting/t-cy/Default_en.asp accessed on 30 September 2012

Criminal Code Act 1995 (Cth)

Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002 (Cth)

Cybercrime Act 2001 (Cth)

Cybercrime Legislation Amendment Bill 2011(Cth)

Department of the Prime Minister and Cabinet. (2012). *The National Security and International Policy Group Executive*. Retrieved from http://www.dpmc.gov.au/national_security/index.cfm#cyber accessed on 30 September 2012

Fildes, J. **(**Technology Reporter), (2010, September 23). *Stuxnet worm 'targeted high-value Iranian assets*, BBC News, Retrieved from http://www.bbc.co.uk/news/technology-11388018 accessed on 30 September 2012

Former Minister for Foreign Affairs. (2011, September 15). *Release of discussion paper on Cyber White Paper* [Press release]. Retrieved from http://www.foreignminister.gov.au/releases/2011/ accessed on 30 September 2012

Grabosky, P. and Stohl, M., "Cyberterrorism" (2003) 82 Reform 8. Retrieved from http://www.alrc.gov.au/reform-journal accessed on 30 September 2012

International Atomic Energy Agency, *Summary of IAEA TM on "Newly Arising Threats in Cyber Security of Nuclear Power Plants" - 23rd TWG-NPPIC, May 26 May 2011*. Retrieved from http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/Day-3.Thursday/TWG-NPPIC-IAEA-TM-Overview.pdf accessed on 30 September 2012

Latimer, P. (2012). Australian business law (31st ed.). Sydney: CCH.

Mele, S. (2010). *Cyberwarfare and its damaging effects on citizens*, Retrieved from http://www.stefanomele.it/publications/dettaglio.asp?id=185 accessed on 30 September 2012

North Atlantic Treaty Organization [NATO], (2012). NATO rapid reaction team to fight cyber attack. Retrieved from http://www.nato.int/cps/en/natolive/news_85161.htm accessed on 30 September 2012

Organization of the Islamic Conference [OIC], (1999). *Convention of the organization of the Islamic conference on combating international terrorism*, Retrieved from http://www.oic-oci.org/english/convenion/terrorism_convention.htm accessed on 30 September 2012

R v Boden [2002] QCA 164.

Robinson, M. (2012, June 26). Cyber terror threat to UK is on an 'industrial scale', says MI5 chief as he reveals one company lost £800 MILLION as a result of state-sponsored espionage. *Mail Online.* Retrieved from www.dailymail.co.uk accessed on 14 November 2012

Security Legislation Amendment (Terrorism) Act 2002 (Cth)

Smith, M. (2010), Counter-Terrorism Committee Executive Directorate (CTED), Retrieved from http://www.un.org/News/briefings/docs/2010/101201_CTED.doc.htm accessed on 30 September 2012

Suppression of the Financing of Terrorism Act 2002 (Cth).

Symantec, *W32.Stuxnet*. 17 September 2010. Retrieved from http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. accessed on 30 September 2012

Telecommunication Interception Legislation Amendment Act 2002 (Cth).

The Sydney Morning Herald [SMH], (2007). *Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks*. Retrieved from http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html accessed on 30 September 2012

United Nations, n.d. UN Action to Counter Terrorism. Retrieved from http://www.un.org/terrorism/ accessed on 30 September 2012