UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30
Issue 1 *2013*

Article 3

2013

Crisis on Impact: Responding to Cyber Attacks on Critical Information Infrastructures, 30 J. Marshall J. Info. Tech. & Privacy L. 31 (2013)

Eugenia Georgiades

William Caelli

Sharon Christensen

W.D. Duncan

CRISIS ON IMPACT: RESPONDING TO CYBER ATTACKS ON CRITICAL INFORMATION INFRASTRUCTURES

EUGENIA GEORGIADES, WILLIAM J. CAELLI,
SHARON CHRISTENSEN, & W.D. DUNCAN*

ABSTRACT

In the developing digital economy, the notion of traditional attack on enterprises of national significance or interest has transcended into different modes of electronic attack, surpassing accepted traditional forms of physical attack upon a target. The terrorist attacks that took place in the United States on September 11, 2001 demonstrated the physical devastation that could occur if any nation were the target of a large-scale terrorist attack. Therefore, there is a need to protect critical national infrastructure and critical information infrastructure. In particular, this protection is crucial for the proper functioning of a modern society and for a government to fulfill one of its most important prerogatives – namely, the protection of its people. Computer networks have many benefits that governments, corporations, and individuals alike take advantage of in order to promote and perform their duties and roles. Today, there is almost complete dependence on private sector telecommunication infrastructures and the associated computer hardware

* Eugenia Georgiades, Associate Lecturer QUT School of Accounting, Doctorate Candidate Griffith University, Bachelor of Arts (Honours), LLB, Grad Dip Legal Practice, LLM. Emeritus Professor William J. (Bill) Caelli, was the A.O. Director of International Information Security Consultants and an Adjunct Professor at Griffith University and Queensland University of University, Australia. Professor Caelli has fifty years of experience in the information technology industry with some forty years of that in the cybersecurity area. He has a Ph.D. in nuclear physics with an emphasis on very high-speed data acquisition systems. He served on Australia's Trusted Information Sharing Network (TISN) from its formation by Australia's Federal Government until 2012 and has participated in major cyber policy activities for over thirty-five years. Sharon Christensen is a Gadens professor of law and teaches property law. She is also a director at Commercial and Property Law Research Centre. W.D. Duncan, LLB, (Queensland), LLM.(London), Professor, Faculty of Law, Queensland University of Technology.

and software systems.[1] These infrastructures and systems even support government and defense activity.[2] This Article discusses possible attacks on critical information infrastructures and the government reactions to these attacks.

I. INTRODUCTION

The rapid progression of technology has allowed for a shift in national information infrastructures (these infrastructures are a subsection of critical national infrastructure as a whole) to information technology and associated systems based on internet protocol. This change has led to an explosion of internet-based businesses, in addition to internet-enabled businesses. Further, this development has transcended into e-government departments and their efficiencies. Corporations, small business enterprises, governments, and individual users use the Internet to transact with customers and/or clients. Additionally, these parties use the Internet to employ efficient work practices that enable them to transact effectively at a minimal cost and to store large amounts of data electronically onsite or off-site.[3] At the same time, military forces have become "digitized" with command, control, and communication centers that revolve around digital systems that may themselves become part of the weapons and defense shields of national military forces. An article in *The Economist* stated this idea simply that "the spread of digital technology comes at a cost: it exposes armies and societies to digital attack."[4] Essentially, the use of electronic communication information systems provides many advantages and disadvantages for governments, which centers around those computer networks and information systems that can be used to facilitate attacks on other information systems.

Global computer networks demonstrate the transnational and borderless way in which nations, corporations, and individuals communicate, as well as the alarming possibilities that attacks on the infrastructure of any nation can be implemented via these same computer technologies. A physical attack, such as a terrorist organization's bombing attack on a nation, is no longer the most viable option for that terrorist organization to disrupt the nation. Now, terrorist groups, criminal organizations, and individuals may carry out digital attacks using computer and data network technologies that may have the same

---

1. CLAY WILSON, CONG. RESEARCH SERV., RL 32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 1 (2008).

2. *Id.*

3. In particular, the emergence of cloud computing has the potential to minimize even further the cost of data storage by businesses off site.

4. *Estonia and Russia: A Cyber-riot*, ECONOMIST (May 10, 2007), http://www.economist.com/node/9163598.

detrimental impact as that of a bomb hitting a nation.[5]

This is demonstrated by the recent increase in cyber attacks.[6] Attacks on the government or the military information systems may potentially fall under one of three categories: cybercrime, cyber terrorism, or cyber warfare. Although there are few examples of legal enforcement against cyber attacks, two recent cyber attacks are significant on the national level – the Estonian Russian cyber attack and the cyber attack on the Australian Maroochy Shire Council's sewerage plant by a disgruntled employee/contractor. Taken together, these examples demonstrate the different aspects of the same problem (i.e. denial of service v. intimidation).

For example, the Australian government's Cyber Security Strategy prioritizes the need to improve the detection, analysis, and response to cyber attacks, focusing on its critical infrastructure. However, responses by individuals, corporations, or the government to cyber attacks must be justified by an appropriate legal and policy framework. This Article will examine through several case studies the legal rights of operators of critical infrastructure (government or corporate) to respond to cyber attacks under the current legal framework. To do so, this Article will highlight by way of the case studies the need to distinguish between crimes, terrorism, and acts of war in order to develop an appropriate response strategy. In particular, this Article will examine if, and when, a retaliatory cyber response is an acceptable legal response.[7]

II. LEGAL NATURE OF CYBER ATTACKS

There are no formal definitions for the terms "cyber attack," "cyber war," or "cyber warfare." At the same time, there are also no formal definitions for a "cyber weapon" or a "cyber munition." Therefore, distinguishing between attacks that constitute a crime, an act of terrorism, and an act of warfare is extremely difficult.[8] Michael Vitas describes

---

5. *Id.*

6. *Id.*

7. This Article does not, however, discuss the current problem of limitation of cyber weaponry or its development, maintenance and usage, nor the potential global efforts towards international agreements in this area.

8. These terms have been used interchangeably; however, each has a subtle difference. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogising Cyber Attacks in International Law,* 27 BERKELEY J. INT'L LAW 192, 199 (2009); *see* Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom Up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275, 275-95 (2009); *see also* Natasha Solce, *Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 300-02 (2008); *see* Richard W. Aldrich, *How Do You Know You Are At War In The Information Age?*, 22 HOUS. J. INT'L L. 223, 224-63 (2000); *see* Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F.L.REV. 122, 125-28 (2009); *see also* Matthew Hoisington, *Cyberwarfare And The Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L

cyber attacks as "computer to computer attacks carried out to steal, erase, or alter information, or to destroy or impede the functionality of the target computer system."[9] This definition of cyber attacks may indicate the commission of a crime or, depending upon the purpose of the attack and its perpetrators, even terrorism or an act of war. The number of possible definitions demonstrates the colloquial and ever-changing nature of the terminology, which bears only a superficial connection to the related legal terminology. For example, the term "cyber attack" may be used to describe cyber terrorism, information warfare, or cyber warfare.[10] Thus, depending on the context and purpose of an attack, the legal ramifications may be conviction of a crime, an act of terrorism, or an act of war.

Further, the term "information warfare" may be used to describe an attack that bears a military character, or more generally, an action intended to "protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."[11] Such attacks may be mounted against civilian, government, or military targets. If the more general definition of information welfare is used, the legal outcome may be the act of a crime or, depending on the country and legislative provisions, an act of terrorism. This indiscriminate use of language to describe such attacks makes development of a legal framework difficult. The legal ramifications and potential response to a cyber attack on critical infrastructure, particularly in the form of a "denial of service" attack (DoS),[12] depends not on its name, but upon a clear understanding of the underlying legal nature of any attack. The legally acceptable response

---

& COMP. L. REV. 439, 439-54 (2009); Jason Barkham, *Information Warfare and International Law on The Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 60-113 (2002); *see also* Christopher M. Petras, *The Use of Force in Response to Cyber Attack on Commercial Space Systems – Reexamining 'Self Defense' In Outer Space In Light of the Convergence of U.S Military and Commercial Space Activities*, 67 J. AIR L. & COM. 1213, 1220-68 (2002).

9. Michael Vitas, *Cyber Attacks: Protecting America's Security against Digital Threats* (John F. Kennedy Sch. of Gov't, Harvard Univ. Discussion Paper No. ESDP 2002-04, June 2002).

10. *See generally,* Solce, *supra* note 8.

11. Richard M. Crowell, *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare* 1, http://www.carlisle.army.mil/DIME/documents/War%20in%20the%20Information%20Age%20%20A%20Primer%20for%20Cyberspace%20Operations%20in%2021st%20Century%20Warfare%20-%20R%20M%20%20Crowell.pdf (last visited Dec. 1, 2013) (citing WINN SCHWARTAU, INFORMATION WARFARE: CYBERTERRORISM PROTECTING YOUR PERSONAL SECURITY IN THE INFORMATION AGE 8-14 (2nd ed. 1996); Blaise Cronin & Holly Crawford, *Information Warfare: Its Application in Military and Civilian Contexts*, 15 INFO. SOC'Y J. 257, 257-63 (2002).

12. A DoS can be carried out by trojan horses, logic bombs, viruses, worms, distributed denials of service, or code breaking. *See* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 STANFORD J. INT'L L. 207, 208 (2002).

by the owner of critical infrastructure to a cyber attack will differ greatly depending upon its legal categorization as a crime, an act of terrorism, or an act of war.

To highlight the distinctions, this Article will use the well-known example of the Maroochy case as a case study of a cyber attack on critical infrastructure.

III. THE MAROOCHY CASE[13] – ATTACK ON CRITICAL INFORMATION INFRASTRUCTURE

In the *Maroochy* case, the defendant was an engineer previously employed for two years by Hunter Watertech, an Australian company, up until he resigned in December 1999. Hunter Watertech was engaged by the Maroochy Shire Council in Queensland, Australia to install wireless systems to monitor and control sewerage and waste water systems. Specifically, the company was contracted to install a "PDS Compact 500" computer system capable of receiving instructions from a central control facility. The system would also allow for the transmission of alarm signals and other data from the sewerage infrastructure to the central computers, as well as providing messages from the central system to stop and start the pumps at associated pumping stations.

After the defendant resigned from the company in December 1999, he directly approached the Council twice for employment, but he was refused. Shortly after January 2000, the sewerage system began experiencing a myriad of faults and difficulties such as: (i) the pumps were not running as they were supposed to; (ii) pump alarms were not communicating to the central computer; and (iii) a failure of communication between the central computer and other pumping stations. Hunter Watertech appointed an employee to investigate the problem. This employee concluded that the technical problems that the computer system was experiencing were due to human intervention rather than failure of the computer equipment.

This investigation entailed the monitoring and recording of all signals, messages, and traffic on the associated wireless data network. The evidence relied upon by the prosecutors demonstrated that: (i) the Council's sewerage system had approximately 150 stations pumping sewerage to treatment plants; (ii) each of the pumping stations had installed a PDS Compact 500 computer that was capable of receiving instructions from a central computer and providing messages to stop and start the pumps at the pumping station; (iii) the pumps were controlled electronically and all communications between the pumping stations and the central computer were by a private two-way radio system operating through repeater stations with each repeater station transmitted

13. *R v Boden*, [2002] QCA 164 (Austl.).

on a different frequency; and (iv) after investigation, pumping station no. 14 appeared to be the source of false messages and that the address of the false messages was PDS Compact 500 computer 14.

To assist in identifying the person responsible for the attacks, the company changed the identification number of pumping station no. 14 to pumping station no. 3 so that any legitimate messages from that station could be identified as originating from that station, now known as station no. 3. Similarly, any messages that were transmitted from a station with identification no. 14 would now be fake. Station no. 14 would be a "bogus" station. A malfunction occurred on March 16, 2000. Communication was sent over the network from the bogus pump station that was apparently sending messages in order to corrupt the system. There was only partial success in changing the program to exclude the bogus messages. The attacker was using PDS ID number 1 to send the corrupt messages. During this time, further problems arose as a result of the intruder gaining remote access to the system, such as the alteration of data so that whatever function was scheduled to occur at a specific time at affected pumping stations did not eventuate or it occurred in a different way than it would have occurred without malicious interference. The effect of this was that the central computer systems were not able to exercise control and technicians had to be stationed at various points to correct the faults that were affecting the various pumping stations. Despite these efforts by the technicians, a pumping station overflowed, causing raw sewerage to escape.

Later, another incident occurred that involved a series of electronic messages disabling alarms at four pumping stations using ID pumping station 4. At this time the defendant was apprehended by police with a PDS Compact 500 computer in his possession.

A. WAS THE MAROOCHY CYBER-ATTACK A CRIME?

The defendant used a computer to interfere with the operation of critical infrastructure, namely pumping systems. This interference caused financial loss to the Council and damage to the waterways by the release of sewerage, along with the associated health risks. Clearly, if the defendant had used physical means to cause damage to the associated infrastructure, his actions would have been a crime due to the obvious physical damage to property. Did the actions of the defendant involve criminal conduct punishable by law?

Cybercrime has no consistent statutory definition and can be used to refer broadly to an "array of criminal activity including offenses against computer data and systems, computer-related offenses, content

offenses, and copyright offenses."[14] In theory, any criminal activity involving the use of a computer or information technology may be a cybercrime. Clearly, therefore an activity, which targets computers themselves, and seeks to destroy or alter information or data held in them, sometimes with a view to interfering in the processes governed by that data, should be described as a cybercrime.[15]

The defendant was prosecuted and convicted prior to the amendments to the Australian *Criminal Code Act 1995*, which added computer crimes to Pt 10.7 of the Act[16] or of obtaining or dealing with identification information pursuant to Section 408D of the *Criminal Code 1899*. If the defendant were prosecuted now, it is likely that pursuant to Section 101.1 of the *Criminal Code Act 1995*, his unauthorized interference with, modification of data on, or impairment to, the operation of a computer would be prosecuted.[17] The offenses of unauthorized modification of data to cause impairment[18] and unauthorized impairment of electronic communication[19] are both broad enough to encompass the type of attack that occurred in the town of Maroochydore located in Queensland, Australia, as well as any DoS attack on any computer or computer system, including those incorporated into critical infrastructure, provided the offense occurs using the Internet.

B. AFTER 9/11 WOULD THE MAROOCHY CASE BE CONSIDERED AS CYBER-TERRORISM?

Since the September 11, 2000 attacks in New York, various legislative amendments have been made to the *Criminal Code 1995* incorporating definitions for computer related offenses and terrorism. If the *Maroochy* case were prosecuted post-2001, it is likely that the *Criminal Code Act 1995* would have been used and not the Queensland Criminal Code. The prosecution could have proceeded as a computer offense (and therefore a crime) or terrorism due to the target of the attack being accepted as "critical" infrastructure. Whether a claim of terrorism would have succeeded is examined below.

---

14. *Crime Types - Definitions and General Information*, AUSTRALIAN GOVERNMENT – AUSTRALIAN INSTITUTE OF CRIMINOLOGY (July 18, 2011), http://www.aic.gov.au/crime_types/cybercrime/definitions.aspx.

15. *Id.*

16. This part was added by the *Cybercrimes Act 2001* (Cth) (Austl.).

17. *Criminal Code 1995* (Cth) pt 10.7 (Austl.). This part was added by the *Cybercrimes Act 2001* (Cth) (Austl.). There are various other offenses that may also apply under state and territory legislation or other commonwealth legislation, such as *Privacy Act 1988* (Cth) (Austl.), *Telecommunications Act 1997* (Cth) (Austl.), and *Telecommunications (Interception) Act 1979* (Cth) (Austl).

18. *Criminal Code 1995* (Cth) s 477.2 (Austl.).

19. *Criminal Code 1995* (Cth) s 477.3 (Austl.).

Various definitions of cyberterrorism have been proffered by commentators, which include:

- a criminal act perpetrated by the use of computer and telecommunications capabilities resulting in violence, destruction and/or disruptions of services to create fear by causing confusion and uncertainty within a given population with the goal of influencing a government or population to conform to a particular political, social or ideological agenda.[20]
- "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[21]
- an attack that "destroys computerized nodes for critical infrastructures such as the Internet, telecommunications or the electric power grid, without ever touching a keyboard."[22]

Under the *Criminal Code Act 1995* ("CCA"), terrorism includes activities that interfere with, disrupt or destroy an electronic system. This same activity will also be captured under the umbrella of cybercrime[23] and the computer offense provisions of the CCA.[24] The difference, however, lies in the purpose and intended outcome from the activity. A "Terrorist Act" is defined in Section 100.1 of the CCA to mean:

> An action or threat of action where:
> (a) the action falls within subsection (2) and does not fall within subsection (3); and
> (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.
>
> Action falls within subsection (2) if it:
> (a) causes serious harm that is physical harm to a person; or
> (b) causes serious damage to property; or

---

20. Vitas, *supra* note 9.

21. Dorothy E. Denning, *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* NETWORKS AND NETWARS 241 (John Arquilla & David Ronfelt eds., 2001); *see also* Dorothy E. Denning, *Is Cyber War Next?*, SOCIAL SCIENCE RESEARCH COUNCIL (Nov. 1, 2011), http://www.ssrc.org/sept11/essays/denning.htm.; WILSON, *supra* note 1.

22. Don Verton, *Sidebar: A Definition of Cyber-Terrorism*, COMPUTERWORLD (Aug. 11, 2003), http://www.computerworld.com/securitytopics/security/story/010801,83843,00.html; *see also* WILSON, *supra* note 1.

23. *See also* WILSON, *supra* note 1.

24. *Criminal Code 1995* (Cth) pt 10.7 (Austl.).

(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.

Action falls within subsection (3) if it:
(a) is advocacy, protest, dissent or industrial action; and
(b) is not intended:
(i) to cause serious harm that is physical harm to a person; or
(ii) to cause a person's death; or
(iii) to endanger the life of a person, other than the person taking the action; or
(iv) to create a serious risk to the health or safety of the public or a section of the public.[25]

If the facts in the *Maroochy Case* occurred today, prima facie the attacker committed an act of terrorism within Section 100.1(2) because he seriously interfered with or seriously disrupted an electronic system used for an essential public utility. It is not necessary under subsection (2) for the attacker to have intended to cause physical injury, property damage, or other economic loss. To negate the allegation of terrorism, the attacker would need to argue: (i) the interference with the electronic system fell within subsection (3); (ii) there was no intention of advancing a political, religious, or ideological cause; and (iii) the act was not done for the purpose of intimidating the government or the public.

It is unlikely that the attacker would have succeeded in proving the conduct was within subsection (3). His conduct was not aimed at industrial action, protest or advocacy for any particular cause, and arguably, the outcome (intended or not) of disrupting a sewerage system is likely to be a public health issue. Clearly though the attacker did not intend to advance a political, religious, or ideological cause. His conduct was retaliatory in nature for the council failing to offer him a job. There also appeared on the facts to be a lack of the necessary intent to intimidate.

---

25. *Criminal Code 1995* (Cth) pt 100.1 (Austl.).

Several interim points can be made about the application of the terrorist provisions of the CCA to an attack on critical infrastructure. A terrorist attack on an electronic system:

° must seriously interfere with, seriously disrupt, or destroy the electronic system;
° does not have to be facilitated by the Internet but can be undertaken internally;
° does not require the person to intend to cause personal injury, property damage, or economic loss;
° is not limited to critical infrastructure operated by government and will extend to an attack on information infrastructure for essential services (water, power, telecommunications, finance, transport) operated by private or semi-government bodies); and
° must advance a political, religious, or ideological cause with the intend of intimidating the government or section of the public.

IV. CYBER TERRORISM CASE STUDY 1 – ESTONIA

In 2007, government, banking, and police systems in Estonia[26] were attacked by a distributed denial of service (DDoS) attack.[27] These attacks starkly demonstrated the effect of a properly and specifically targeted cyber attack on the critical information infrastructure of a country. The attacks not only caused a breakdown in critical systems (banking, telecommunication, and government offices)[28] but also precipitated riots and internal conflict. The attacks were carried out through a DDoS implemented by the placement and use of "botnets" to overload the system, which "lasted from anywhere between one to ten hours and originated from a diversity of countries such as Egypt, Peru, and

---

26. Duncan B. Hollis, *Why States Need An International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1025 (2007); *see also* Jurich, *supra* note 8, at 275; Solce, *supra* note 8, at 305.

27. *See generally*, Sharon Christensen, et al., *An Achilles Heel: Denial of Service Attacks on Australian Critical Information Infrastructures*, 19 INFO. & COMMC'NS TECH. L. 1 (2010); *see also* Shackelford, *supra* note 8, at 204 (explaining that "DDoS attacks aim to crash a target site by bombarding it with bogus requests for information"); *Estonia and Russia: A Cyber-riot*, *supra* note 4; Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies,* 24 CARDOZO ARTS & ENT. L. J. 23, 26 (2006) (asserting that DoS attacks are "almost always mounted as distributed denial of service attacks which work by using remotely controlled computers to generate more requests of a device than it can serve").

28. Hollis, *supra* note 26; *see also* Jurich, *supra* note 8; Robert Vamosi, *Cyberattack in Estonia - What It Really Means*, CNET (May 29, 2007), http://news.cnet.com/ Cyberattack-in-Estonia-what-it-really-means/2008-7349_36186751.html; Shackelford, *supra* note 8; Aldrich, *supra* note 8; Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUROPEAN J. INT'L L. 825, 825-65 (2001).

Russia."[29] It has been suggested that 128 DDoS attacks targeted Internet protocol-based data networks and computer systems during the attack period on Estonia.[30] DDoS attack vectors are commonly used to mount cyber attacks, and this attack was not the first one of its kind against a country.[31]

A. HOW DID THE ESTONIAN GOVERNMENT DEAL WITH THE ATTACKS?

The attacks were so severe that Estonia had considered invoking Article 5 of the North Atlantic Treaty, which provides that an attack on one allied country compels the alliance to attack the aggressor country.[32] An investigation undertaken after the attack by Estonian officials claimed to reveal evidence that Russia, as a nation state, was behind the attacks. [33] The difficulty faced by Estonia in proving this claim was that most of the attacks occurred through a "botnet"[34] using private and untraceable computers globally. A "bot" is essentially a type of "malware that is installed into a compromised computer which can then be controlled remotely by a botmaster for executing some orders through the received commands."[35] The complex architecture of a DDoS complicates the process of tracing the source of a cyber attack.

B. HOW DID ESTONIA RESPOND?

The difficulty of proving an attack by Russia led Estonia to undertake a preservation and containment response by shutting down its networks; and in addition, to seek investigative help from the United States.[36]

---

29. Shackelford, *supra* note 8, at 204.

30. *Id.*; *see also* Sean Michael Kerner, *Estonia Under Russian Cyber Attack?*, INTERNETNEWS.COM (May 18, 2007), http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm.

31. Shackelford, *supra* note 8, at 204.

32. *See* North Atlantic Treaty art. 5, Apr. 4, 1969, 63 Stat 2241, 34 U.N.T.S 243; *see also* Shackelford, *supra* note 8, at 204.

33. Shackelford, *supra* note 8, at 207.

34. "A botnet is a type of malware which is installed into a computer that is comprised of, and can be controlled by, a Botmaster. Once the Bot code has been installed, the compromised computer becomes a Bot or a Zombie, which is used by the Botmaster to attack. Botnets are networks comprised of a large number of Bots. Botnets are created to set up a private communication infrastructure which can be used for malicious activities such as DDoS by the Botmaster." Hossein Rouhani Zeindaloo & Azizah Bt Abdul Manaf, *Botnet Detection by Monitoring Similar Communications Patterns*, 7 INT'L J. COMPUTER SCI. INFO. SEC. 36, 36 (2010).

35. *Id.*

36. *Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008*, U.S. CYBER CONSEQUENCES UNIT (Aug. 2009), *available at* http://www.registan.net/wpcontent/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

V. CAN A CYBER ATTACK ON CRITICAL INFRASTRUCTURE BE AN ACT OF WAR?

A. CONCEPTS OF ARMED ATTACK, USE OF FORCE, AND ACT OF WAR: WHAT'S THE DIFFERENCE?

"An act of war is an action by one country against another country with the intention of provoking a war, or an action that occurs during a declared war or armed conflict between military forces of any origin."[37] The extension of the term information warfare or "cyber war" beyond a military context to define cyber interference or conflicts of a corporate or more general nature contributes to the confusion in terminology.[38] Indeed Clarke and Knake adopt their own definition as referring to "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption."[39] At the same time, penetration of the information infrastructure of a nation by any entity may occur for a number of reasons, such as creating an advantage, exerting influence, projecting an impression of power of one state over another, and so on. These concerns are referred to by Kugler in consideration of the needs for deterrence of any form of cyber attack.[40] They illustrate the problem of definition by reference to alleged cyber-oriented disruption of defense-related radar surveillance systems of one nation by another. Complexity occurs here as definitions of "electronic warfare" may also be involved which may lay outside the use of computer systems, e.g. "jamming" of wireless signals, overpowering and takeover of TV transmissions, etc. This all may be seen as a military related activity against national defense forces by other military forces or national intelligence entities. However, the majority of suspected information warfare type attacks on corporate or general commercially oriented, government systems must be classified as crimes or acts of terrorism or intimidation. The broad definition of information warfare is "the use of information or information technology during a time of crisis or conflict to achieve or promote specific objectives over a specific

---

37. *Act of War Law & Legal Definitions*, USLEGAL, http://definitions.uslegal.com/a/act-ofwar/ (last visited Dec. 1, 2013).

38. Kenneth J. Knapp & William R. Boulton, *Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments*, INFORMATION SECURITY TODAY 76 (spring 2006), http://www.infosectoday.com/Articles/cyberwarfare.pdf; *see also* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J. L. TECH. & POL'Y 1, 1 (2002).

39. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 11 (2010).

40. *See* Richard. L. Kugler, *Deterrence of Cyber Attacks, in* CYBERPOWER AND NATIONAL SECURITY (Franklin D. Kramer, Stuart H. Starr, & Larry Wentz eds., 2009).

adversary or group of adversaries"[41] is sufficiently broad to encompass crimes, terrorism, or acts of war. Thus, what will distinguish an act of war from simple crimes or acts of terrorism? As an adjunct to this discussion, the concept of cyber "munitions" arises with the associated concept of "arms control" for cyberspace as any cyber attack presupposes the existence of such systems.

It is submitted that cyber warfare should be limited to "a hostile attack by one nation against the important IT systems [critical infrastructures] and networks of another (as compared to a criminal or terrorist attack involving private parties)."[42] This would extend to attacks by one nation state against another nation state with the aim to incapacitate or severely debilitate telecommunications, "electrical power systems, gas and oil storage, transportation, banking and finance, military forces and emergency services including medical, police, fire and rescue to use or manage that network."[43]

The proposed meaning of cyber warfare (as an act of war) is extended to encompass attacks upon any infrastructure that is owned and operated by the private or public sector and which is considered to be of national significance, not being limited to specific military infrastructure. Importantly the term should be restricted to acts by other nations and not to politically or religiously motivated attacks by individuals or groups. This consideration has been emphasized by the report of the "Perfect Citizen" project in the United States whereby that nation's National Security Agency (NSA) would actively assist in monitoring the data networks of critical infrastructure operators in that nation in order to assist in detecting any cyber attack.[44] The report stated that it would "detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants."[45]

That type of activity would fall within the concept of terrorism. However, is it possible for an operator of critical infrastructure to distinguish between them? Should the distinction be made on the identity of the attacker (individual/nation state); the type and significance of the

---

41. *Information Warfare*, FREEDICTIONARY.COM, http://www.thefreedictionary.com/Information+operation (last visited Dec. 1, 2013). There are many different definitions of information warfare but for the purposes of this paper, a simplistic one will be sufficient to demonstrate the distinction between cyber warfare. *See* Solce, supra note 8, at 300; *see* Cronin & Crawford, *supra* note 11, at 257; *see* Jensen, *supra* note 12, at 207; *see* Shackelford, *supra* note 8; *see* Jurich, *supra* note 8.

42. Shackelford, *supra* note 8.

43. Todd A. Morth, Note, *Considering Our Position: Viewing Information Warfare as A Use of Force Prohibited by Article 2(4) of the UN Charter*, 30 CASE W. RES. J. INT'L L. 567, 571 (1998).

44. Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, WALL ST. J. (Jul. 8, 2010), http://online.wsj.com/news/articles/SB10001424052748704545004575352983850463108.

45. *Id.*

electronic system attacked (critical infrastructure/corporate system); the extent of the attack (several critical systems/only one system, repetitive attacks/single attack); or the impact of the attack (destruction of system, incapacity of system for a short time). The real problem, however, is one of attribution. The question is one, moreover, of determination of just what is meant by an "act of a nation" as distinct from any other entity. This can be even further complicated if it is considered that individuals or groups may operate and perform such cyber attacks with or without the explicit permission or organization of the nation state representatives. The emphasis here is one of "asymmetry" in that, unlike conventional warfare, the equivalent "cyber munitions" may be readily developed or obtained by any person or group, IT expert or amateur alike. Indeed, such cyber munitions may be readily and freely available from sources connected to the global Internet.

The importance of distinguishing between terrorism and an act of war lies in the identification of the set of permissible responses. An act of war may justify a retaliatory attack on the critical infrastructure of the attacking nation, but an act of terrorism does not. Retaliatory action taken by a national state to defend its systems may also be an act of war unless justified by the prior attack.[46] Careful consideration is therefore necessary prior to responding to an attack by then attacking the infrastructure of another country. Several examples of cyber attacks on national infrastructure with potential attributes of an "act of war" are explored in the next part of this Article. This part will demonstrate the difficulties faced by governments in ascertaining the source of a potential "act of war" cyber attack, resulting in a response aimed at preservation and containment of the attack rather than retaliation. However, the determination to create suitable response mechanisms to cyber attack has been referred to by the U.S.'s CNCI as those responses " . . . aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses by both state and non-state actors."[47] At the same time, the formation of the DoD "Cyber Command" under the control of a four star General, who also heads the U.S.'s National Security Agency, indicates that cyber warfare is being closely examined today.[48]

---

46. Shackelford, *supra* note 8.

47. *The Comprehensive National Cybersecurity Initiative*, OFFICE OF THE PRESIDENT OF THE UNITED STATES, *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (last visited Dec. 1, 2013).

48. "National Security Agency (NSA) Director Keith Alexander has been confirmed by the Senate to lead the Defense Department's new Cyber Command, which will integrate the military's offensive and defensive cyber capabilities. In approving Alexander to head the command on May 7, senators agreed by a voice vote to elevate Alexander, previously an Army lieutenant general, to a four-star general." Ben Bain, *Senate Confirms*

It is imperative to note that, from a national security point where a country's infrastructure has been attacked, it is useful to consider the United Nations Charter's term "Use of Force."[49] Commentators have asserted that "under the current international law, if a Computer Network Attack rises to the level of a 'use of force,' the victim nation may have a broader range of options than if it does not constitute a use of force."[50] There may be other avenues of pursuing without reacting in line with the "use of force." The Law of Armed Conflict (LOAC) provides little clarification of the issue, since there is uncertainty as to whether "an Information Operation (IO) is an act of war which is determined by the nature of the activity."[51] The discrepancies between the various international legal instruments and convention have only widened the ambit of confusion in relation to what constitutes as an act of war or use of force. Traditionally these conventions were drafted in times when the importance of computer and network security was not foreseeable.[52]

Subsequently, the definition of "war" is defined by the LOAC as "warfare by a belligerent nation involving actual arms . . . weapons that deploy kinetic energy to cause the enemy some form of physical damage."[53] Commentators have argued that "electrons and binary digits floating through computer networks and into another computer is *not* the equivalent of armored division rolling across a national border."[54] While this argument has some merit, there is the counter argument that the electrons and binary digits floating through computer networks to attack other computers may fall within the second limb of a very crude test, *viz*. which is to cause the enemy some form of physical damage. If the CNA targets the telecommunication information infrastructure being attacked and there is no telephone to call, emergency services would have a significant impact on the people of the nation being attacked. In simple terms, the concept and definition of "cyber weapons," "cyber munitions," and their deployment are unclear.

The LOAC test is that firstly, weapons using "kinetic energy" must be used. Secondly, it must cause the enemy some form of physical damage. From this viewpoint, the use of "electromagnetic energy" to disrupt communications and computer systems seems outside the definition, yet such activity, e.g. jamming of radio/TV broadcasts, disruption of radar surveillance facilities and the like, have been reported for decades.

NSA Chief as Head of Pentagon's New Cyber Command, FED. COMPUTER WKLY. (May 11, 2010), http://gcn.com/gig/gigshared/blogs/cybersecurity/2010/05/alexanderconfirmation.aspx.

49. *See* Jensen, *supra* note 12, at 214.

50. *Id.*

51. David J. DiCenso, *Information Operations: An Act of War?*, *available at* http://www.iwar.org.uk/iwar/resources/airchronicles/dicenso1.html.

52. *Id.*

53. *Id.*

54. *Id.*

Whether the foundational basis of the LOAC may still be considered as valid in the current modernity of technological evolution remains unexamined. Examination of the times and context in which these conventions and laws were drafted will demonstrate that they were drafted in times where electronic and digital systems advancement was very limited and unforeseeable.[55]

VI. RESPONDING TO A CYBER ATTACK ON CRITICAL INFRASTRUCTURE

Cyber warfare poses a significant threat to national security and becomes a critical consideration in assessing denial of service concerns at the national level. An attack on a single critical infrastructure can potentially launch further attacks on other interconnected critical infrastructures with unforeseeable consequences for the ability of a nation state to continue operating its telecommunications, financial and commercial sectors, and allied systems. Indeed, an attack on the underlying critical information infrastructure basic to the monitoring and control of all such national infrastructure must be considered of paramount concern. For example, commentators argue that if the:

> attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatch network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots and a political crisis.[56]

Global networks make it easier for terrorist groups and enemy nations to easily and cheaply launch an attack via the Internet using easily accessible tools such as worms, viruses, Trojan horses, logic bombs, trap doors, DoS attacks, and malicious codes, emphasizing again the "asymmetric" nature of the cyber challenge.

The potentially devastating consequences of a coordinated attack on critical infrastructure via the Internet, particularly aimed at denial of service, justifies closer consideration of the potential legal response framework for a suspected cyber attack by one nation state on the critical infrastructure of another.

---

55. *Id.*
56. Jensen, *supra* note 12.

VII. CASE STUDY 2 - GEORGIA

In August 2008, a cyber attack originating in Russia was carried out against Georgian interests via the defacement of public websites. In August 2009, the United States Cyber Consequences Unit (US-CCU) provided a special report of the cyber attack against Georgia in 2008.[57] The US-CCU report provided that in relation to the type and identity of the attacks and attackers:

> ° there was little or no direct involvement by the Russian government or military;
> ° the organisers of the cyber attacks had advance notice of Russian military intentions and they were tipped off about the timing of the Russian military operations while these operations were being carried out;
> ° Social networks operating over the Internet were the main tool used to recruit those carrying out the attacks;
> ° The civilian cyber attackers were aided and supported in their efforts by Russian organised crime;
> ° The total number of individual civilian cyber attackers involved in the campaign against Georgia was much greater than in the campaign against Estonia although the total number of computers involved was much smaller.[58]

It was considered that the first initial attacks were undertaken by botnets and control and command systems[59] that had been used for criminal activities by Russian organized crime.[60] Following the initial attacks, the main type of attack used to expand the overall activity was a series of postings on websites.[61] The US-CCU report states that the "postings contained both the cyber attack tools and the lists of suggested targets for attack."[62] The primary methods of attack were essentially denial of service (DoS) and website defacements,[63] which although simple to execute, were in this case carried out in a sophisticated

---

57. *Overview by the US-CCU, supra* note 36.
58. *Id.*
59. *See also* Zeindaloo & Manaf, *supra* note 34. This Article provides that "botnets are networks comprising of a large number of Bots. Botnets are created to set up a private communication infrastructure which can be used for malicious activities such as DDoS" by the Botmaster, "sending large amounts of SPAM or phishing mails and other nefarious purposes. Bots infect a person's computer in many ways. Bots usually disseminate themselves across the Internet by looking for vulnerable and unprotected computers to infect. When they find an unprotected computer, they send a report to the Botmaster. The bots stay hidden until they are commanded by the Botmaster to perform an attack or task." *Id.*
60. *Id.*
61. *Id.*
62. *Id.*
63. *Overview by the US-CCU, supra* note 36.

manner.[64] The attacks did not result in physical damage to infrastructure or high economic loss indicating the restraint of the attackers. The US-CCU asserts that some of Georgia's critical infrastructures:

> were accessible over the Internet at the time Russia invaded Georgia. There is reason to believe that at least some of these infrastructures would have been vulnerable to cyber attacks causing physical damage. Meanwhile, at least some of the Russian cyber attackers showed signs of considerable technical expertise. If the Russian military had chosen to get directly involved, such attacks would have been well within their capabilities. The fact that physically destructive cyber attacks were *not* carried out against Georgian critical infrastructure industries suggests that someone on the Russian side was exercising considerable restraint.[65]

A. HOW DID GEORGIA RESPOND?

Georgia's first response was to contact Estonian officials who had previous experience with cyber attacks.[66] Like Estonia, Georgia did not have in place a policy or strategy for responding to cyber attacks. The Estonian officials suggested that Georgia contact an informal network of international cyber security experts who could assist in tracing the source of the attack.[67] The second response was technical, aimed at preserving the systems and preventing further attacks. Georgia installed filters to block all Russian IP addresses and the protocols used by the attackers. However, the attackers later circumvented these filters.[68] The attackers used foreign services to disguise their actual IP addresses and attack software that spoofs IP addresses by changing protocols.[69] The most effective technical response was to change the hosting of their websites to other countries where the traffic could be filtered and where greater capacity for access by users of the websites was available. Despite these steps, Georgia found it difficult to maintain access to its websites due to the volume of traffic generated by the attack.[70] A retaliatory attack was performed by Georgia against Russian targets. A counter-attack against Russian websites was mounted through the use of a counter attack tool that had been itself posted on Russian websites, with instructions for Russian sympathizers to use it against Georgia.[71] It has been suggested that damage was limited.

---

64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

VIII. RESPONSES TO CYBER-WARFARE

An attack on national critical information infrastructure by another nation state raises the issue of whether a retaliatory strike by the affected nation is a justified response to an illegal use of force within the meaning of the United Nations Charter or customary international law?[72] Further, could the nation state allege that the attack triggers a right for the nation to defend itself by striking back at the attacker(s) in any way deemed suitable? This question was posed as follows by the United States in 2009, " 'the U.S. military's response to a cyber attack would not necessarily be limited to cyberspace,' the head of U.S. Strategic Command said Thursday. 'The Law of Armed Conflict will apply to this domain,' said Air Force Gen. Kevin P. Chilton. The United States' response to a cyber attack would be decided by the president and Defense secretary, Chilton told reporters during a breakfast roundtable."[73]

As demonstrated by the Estonian and Georgian case studies, while retaliation is often threatened, it is rarely carried out. Retaliation by attacking the electronic systems of another country is of a high risk unless the source of the attack can be absolutely verified and the impact of the initial attack justifies retaliation, i.e. the response is proportionate to the attack. To date these two factors have not been present in documented cyber attacks.[74] For example, attacks on the United States military departments allegedly originating in North Korea have resulted in a lack of retaliation by the United States. This lack of retaliation potentially demonstrates the following:

- The sites attacked represent a low risk to national security;
- The threat was superficial and did not penetrate the system;
- The inability to prove with certainty the origin of the attack contributes to uncertainty about the way in which a country should respond to a cyber attack; and
- An absence of international instruments/treaties dealing with legal responses to cyber attacks by nation states.

---

72. *See* Jensen, *supra* note 12.

73. Jeff Shogol, *Official: No Options 'Off the Table' for U.S. Response to Cyber Attacks*, STARS AND STRIPES (May 8, 2009), http://www.stripes.com/news/official-no-options-off-the-table-for-u-s-response-to-cyber-attacks-1.91319.

74. For example, in 2001 professional Chinese hackers vandalised Japanese company websites and research centres; and in 2009, there were attacks on the Melbourne International Film Festival by Chinese hackers who booked out all film sessions on its website. *Chinese Hackers Attack Film Festival Site,* ABC (Aug. 1, 2009), http://www.abc.net.au/news/2009-08-01/chinese-hackers-attack-film-festival-site/1375162.

IX. INTERNATIONAL POLICIES AND STRATEGIES

The appropriate response to cyber attacks (whether constituting terrorism, criminal activity or an act of war) has been the subject of cyber security/national security strategies and policies in a number of countries. Countries that have adopted cyber attack policies and strategies within military plans include Russia, China, and India.[75] In the United States, the formation of the "cyber command" in 2010 under a four-star general, General Alexander, points to the acknowledgement of the strategic and defense significance of the cyber warfare and allied DoS threats by that country as stated earlier in this Article. Indeed Alexander is reported to have clearly stated the situation in the following terms in June 2010, " 'the U.S. military should be prepared to counter cyber attacks intended to disrupt operations as well as to paralyze and destroy entire computer networks,' the U.S. Cyber Command's new head said today."[76]

A. INDIA

There is little information available in relation to India's approach to the protection of critical information infrastructure systems. The information available is generally broad and fragmented, because India's approach relates primarily to e-commerce. The majority of information in this regard appears to be nationally classified and thus not available. One of the aims of the Indian government was to make India a super power in the knowledge economy by increasing its IT and e-business.[77] The Indian government aimed to achieve this by making India one of the largest producers and exporters of software internationally.[78] In light of this goal, the Indian government established the following to enable it to meet its objectives: National Task Force on Information Technology and Software Development;[79] which had a mandate to create a draft of the National Informatics Policy and prepare recommendations; a vision statement and a policy for incorporation of information

---

75. Jensen, *supra* note 12, at 212; Dan Verton, *Defense Agency, Veridian to Pinpoint Foreign Hackers,* INFOWORLD (Aug. 29, 2001), http://www.infoworld.com/articles/hn/xml/01 /08/29/010829hndefense.xm (discussing Veridian's upcoming contract with the Department of Defense to study computer intrusions and hacks by China against DOD computers); Darcy Noricks, *Cyber Attacks on U.S. Security,* WASH. TIMES (Apr. 20, 2000), http://www.washingtontimes.com/news/2000/apr/20/20000420-011112-9210r/.

76. Tony Cappacio, *Cyber Command Director Alexander Warns of Network "Sabotage,"* BUSINESSWEEK (June 27, 2010), http://www.businessweek.com/news/2010-06-03/cyber-command-director-alexander-warns-of-network-sabotage-.html.

77. ELGIN M. BRUNNER & MANUEL SUTER, INTERNATIONAL CIIP HANDBOOK 2008/2009, *available at* http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf.

78. *Id.*

79. NATIONAL TASK FORCE ON INFORMATION TECHNOLOGY & SOFTWARE DEVELOPMENT (Jan. 2000), http://www.it-taskforce.nic.in.

technology nationally.[80]

In May 2006 the National E-Governance Plan (NeGP) was approved by the Indian government. The NeGP's role is to create the core infrastructure policies and realize the three elements of e-Governance Plan: data processing centers, State Wide Area Networks (SWANs) and Common Services Centers (CSCs).[81] One of the initiatives established under the NeGP is that standards are vital in ensuring integration and interoperability of data and electronic information.[82] On this basis, the Department of Information Technology (DIT) has established a core group of standards for e-Governance.[83] The Core Group's role was to develop an institutional mechanism and processes, as well as recommending crucial areas for standardization.[84] These areas are as follows:

- Technical standards;
- Localization standards;
- Quality and documentation;
- Security standards; and
- Metadata and data standards for various application domains.[85]

It is noted that the DIT approves and formulates working groups that are representatives of public and private groups, such as associations, industry, academia, and central and state governments.[86] There are white papers which are published through the National Informatics Centre (NIC) which have dual benefits of serving as discussion papers but as well as informing and educating the working groups which develop standards.[87]

The Indian government has the following organizational structure for national security interests. This is a hierarchal structure which begins with the National Information Board (NIB) which is the head of the structure, the National Technology Research Organisation (Technical Cybersecurity) and the National Information Security Coordination Cell (NISCC) have direct links to the NIB but they also form part of the of thee National Security Council Secretariat (NSCS).[88] The NSCS holds instructions to coordinate cyber security activities nationwide and is implemented through the Sectoral Cyber Security Officers

---

80. BRUNNER & SUTER, *supra* note 77.
81. *Id.*
82. *Id.*; *see also* NATIONAL INFORMATICS CENTER, http://home.nic.in (last visited Dec. 20, 2013).
83. BRUNNER & SUTER, *supra* note 77.
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.; see also* NATIONAL INFORMATICS CENTER, *supra* note 87.
88. BRUNNER & SUTER, *supra* note 77.

(SCOs).[89]

Under the NIB comes the Information Infrastructure Protection Center (IIPC), closely followed by the state cyber police stations and then Computer Emergency Response team India (CERT-In), followed by the state and sectoral level CERTs.[90] There have been a number of agencies and centers established in order to support India's information infrastructure protection:

- National Information Board (NIB)
- National Information Security Coordination Cell (NISCC)
- Ministry of Communications and Information Technology (MOC) : Department of Information Technologies (DIT)
- Standardisation, Testing and Quality Certification (STQC) Directorate
- Information Security Technology Development Council (ISTDC)
- Public /Private partnerships between the US and India Cyber Security Forum.[91]

The Indian government, like the United States, United Kingdom and Australia, has also set up a Computer Emergency and Response Team (CERT-In) which responds to computer-related incidents (involving security) by the national computer and networking community.[92] It also functions as an educational forum whereby it raises security awareness among the Indian IT industry. One major distinction between India and other countries is that they have set up five sector specific CERTs which are allocated to the army, air force, navy, banking, and railways. There is an expectation that there will be further CERTs created for the telecom and power sectors.[93]

The Indian government has enacted legislation that deals with information technology as a means of providing the legal framework of recognizing the importance of electronic commerce.[94] There is an Information Technology Act (IT Act) that was enacted in 2000 and amended in December 2009. This Act is extensive and quite original of its kind because it deals specifically with information technology, as well as addressing cyber crime issues and the admissibility of digital evidence.[95] This has been implemented through the amendments of various provisions in other Acts such as the Indian Penal Code 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act 1891,

89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*

and the Reserve Bank of India Act.[96]

The significance of the Indian IT Act is that it is divided into thirteen chapters and ninety-four sections. The chapters relate to various areas of IT, however the following chapters are relevant to the discussion:

- Chapter V- Secure Electronic Records and Secure Digital Signatures;
- Chapter VII Digital Signature Certificates
- Chapter IX Penalties and Adjudication
- Chapter XI Offences
- Chapter XII Network Service Providers Not to Be Liable in Certain Cases;
- There are also IT related offenses contained in the IT Act 2000 which deal specifically with various cyber crime provisions. The following are just a few examples:
  - Hacking and tampering with computer source code;
  - Breach of confidentiality and privacy.

Pursuant to the Penal Code, there are a number of IT related provisions such as forgery (creating false documents or electronic records), cheating, and other issues such as Data Protection and Intellectual property law.[97] Most recently, a new regulatory environment has been approved governing the procurement of ICT systems for use in the national telecommunications and Internet services area where such systems are used by government. The appropriate regulation states as follows: "The service providers shall apply for security clearance for procurement of equipment/software in the proscribed proforma."[98] This is established by the Telecom Regulatory Authority of India (TRAI).[99] This authority was established in 1997 as the private sector entered the telecommunications market in India. TRAI has major recommendatory, regulatory and tariff setting functions in India. The overall security dimensions of this decision were summarized by a report from Indian-Commodity.com as follows:

> The government directed telecom players, both public and private, to get security clearance for obtaining telecom equipment/software from foreign vendors. The directive of the Department of Telecom (DoT) has also made it compulsory for equipment vendors . . . The move is meant

96. *Id.*

97. *Id.*

98. AUSPI NEWS BULLETIN (Feb. 25, 2010), *available at* http://www.auspi.in/news/AUSPI_NEWS_BULLETIN_DEC_2010.pdf.

99. TELECOM REGULATORY AUTHORITY OF INDIA, (Mar. 12, 2013) http://www.trai.gov.in.

> to address concerns raised by security agencies that telecom equipment may carry spyware enabling other countries to snoop into Indian networks.
>
> However, the equipment and software manufactured by Indian companies are exempted from such a necessity . . . As it is one of the effective measures to reduce vulnerability in the long run, the equipment vendors must transfer technology to Indian manufacturers. In case of non-compliance, both vendor and the service provider would be penalized while criminal proceedings would also be started in this case . . .[100]

A clarification of the approach was reported in June 2010 as follows: "A senior official in India's home ministry said under the new proposals, Indian mobile phone operators could import telecom gear from any company after clearing mandatory security checks to be certified by security audit firms such as U.S.–based Infoguard."[101]

A different approach is evident in Australia and the United States. Policies concerning cyber attacks, while relevant to national security, are framed to protect both corporate and government operated critical infrastructure. Consequently, the strategies emphasize the development of resilient information systems with both preventative and responsive capacities.

The Australian Cyber Security Strategy outlines Australia's national approach to cyber security related to infrastructure important to the "national interest."[102] The strategy highlights the international concerns in relation to attacks on critical electronic systems in both government and the private sector as a means for individuals or other nation states to damage Australia's prosperity and national security.[103] The strategy asserts that Australian computers experienced malware infections in 2008 totaling 17,692,587 instances, which "reported the fifth highest level of infections worldwide."[104]

---

100. *Security Clearance for Telecom Equipment Mandatory*, INDIAN-COMMODITY (Mar 23, 2010), http://www.indian-commodity.com/top-news/Security-Clearance-For-Telecom- Equipment-Mandatory.aspx.

101. *Gov't May Allow Chinese Telecom Imports – Source*, YAHOO INDIA (Jun. 3, 2010), http://in.news.yahoo.com/137/20100602/744/tbs-govt-may-allow-chinese-telecom-impor_1.html.

102. This includes the traditional types of critical infrastructure (power, water, aviation, maritime and telecommunications) and other infrastructure of high economic value such as information systems supporting banking and international trade.

103. *See also Cyber Security Strategy*, AUSTRALIAN GOVERNMENT, http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity (last visited Dec. 20, 2013).

104. *Id.*

The strategy emphasizes the need for both commercial and government systems to be secure and resilient. Policies and strategies for supporting this aim center in the establishment of CERT and the Australia and Cyber Security Operations Centre (CSOC). CERT is responsible for coordinating a holistic approach to cyber security across Australia and ensuring a greater understanding and sharing of threats, vulnerabilities, advice, and assistance to corporate Australia. CSOC is responsible for situational awareness of cyber attacks and the coordinating body for cyber attacks on government and critical infrastructure. An important priority of the Strategy is "threat awareness and response" where the Australian government proposes a number of measures:

- establishing a Cyber Security Operations Centre (CSOC) within the Department of Defense to provide a 24/7 cyber situational awareness capability and coordinate responses to cyber security events of national importance;
- creating a new national computer emergency response team, CERT Australia, to share information and improve the coordination of responses to cyber security threats between government and the private sector;
- actively participating in and facilitating trusted and timely information sharing within and between government and business, nationally and internationally, to ensure the maintenance of situational awareness and a consistent, global response to online threats;
- developing an updated cyber security crisis management plan that outlines the arrangements for responding to cyber security events of national significance, including coordination with the States and Territories and the private sector; and
- conducting a program of cyber security exercises to test and refine event response arrangements, including the Cyber Storm series of exercises coordinated by the United States.

The emphasis is on the development of threat assessment measures obviously aimed at preventing an attack. While a crisis management plan is proposed, it is not clear whether the plan proposes preservation and containment or some forms of response or retaliation. This is consistent with the guidelines provided by the Trusted Information Sharing Network for owners and operators of critical information infrastructures for best practices in relation to managing and mitigating risks and threats.[105] For example, the TISN's guidelines for

105. TRUSTED INFORMATION SHARING NETWORK, MANAGING DENIAL OF SERVICE (DOS) ATTACKS (Dec. 2009), *available at* http://www.tisn.gov.au/Documents/ITSEAG

SCADA Security Advice for CEO's "outlines the threats associated with DoS and key issues that CEO's ought to be aware of."[106]

B. UNITED STATES

In the United States, there have been endeavors to establish security measures for the protection of information infrastructures such as banking and finance, power and energy infrastructures information, and other various agencies through the Department of Homeland Security.[107] These endeavors appear to originate in 1997 with the finalization and acceptance of the "Marsh Report" on critical infrastructure protection. In evidence before the United States Congress after submission of the report, Marsh stated as follows:

> My perspectives arise from serving on the Commission, established, as you are aware, by Executive Order 13010 on July 15, 1996. A joint government and private sector endeavor, this Commission was charged to develop a national policy and implementation strategy for protecting our critical infrastructures from physical and cyber threats and assuring their continued operation. The President identified eight infrastructures as our national life support systems: telecommunications, electric power, oil and gas transportation and storage, banking and finance, transportation, water supply systems, emergency services (such as medical, police, fire and rescue), and continuity of government services. These national infrastructures are vital in that their incapacity or destruction would have a debilitating impact on the defense and economic security of the United States. This refers specifically to cyber threats and response to them.[108]

The 2003 National Security Strategy to Secure Cyberspace report established three main objectives, which are as follows: (i) "prevent cyber attacks against critical infrastructures;" (ii) "reduce the U.S. vulnerability to cyber attacks;" and (iii) "minimize damage and recovery time from cyber attacks that do occur."[109]

In 2003, President George Bush stated, "by 2003 our economy and national security became fully dependent upon IT and the information infrastructure. A network of networks directly supports the operation of all sectors of our economy – energy, transportation, finance, banking, information and telecommunications, public health, emergency services, water, medical, defense, industrial trial base, food, agriculture, and

---

+Managing+Denial+of+Service+(DoS)+Attacks++Summary+Report+for+CIOs+and+CSOs.pdf

106. TRUSTED INFORMATION SHARING NETWORK, SCADA SYSTEMS ADVICE FOR CEOS (Mar. 2012), *available at* http://www.tisn.gov.au/Documents/SCADA-Advice-for-CEOs.pdf

107. Knapp & Boulton, *supra* note 38.

109. Critical Infrastructure Protection in the Information Age, 66 Fed. Reg. 53063 (Oct. 18 2001).

109. Knapp & Boulton, *supra* note 38.

postal and shipping."[110] This statement has been observed by the United States' present political agenda for strengthening cybersecurity.

The establishment of the "Cyber Command" in 2010 highlights an interventionist approach to the overall aspect of cyber defense and thus prevention or mitigation of DoS attacks. The United States' cyber command, under the control of a four star general, is directed at protection of military computer systems and networks and the extension of its role into critical infrastructures and non-military government systems. "Most importantly, perhaps, procedures are now being worked out for Cybercom to help the Department of Homeland Security defend government and civilian networks, much like the military contributed to disaster recovery efforts after Hurricane Katrina and the Gulf of Mexico oil spill. In those incidents, it took days, even weeks for the military to fully swing into action. In the event of an information attack, those timelines could be drastically collapsed. There's probably gonna be a very temporal element to it. It's gonna need to be pretty quick," a Cybercom official stated.[111] The National Security Agency is developing threat-monitoring systems for government networks dubbed Einstein 2 and Einstein 3; Deputy Secretary of Defense William Lynn believes those programs ought to be extended to cover key private networks, as well.[112] "We are already using our technical capabilities . . . to protect government networks," Lynn announced at the Strategic Command Cyber Symposium here.[113] "We need to think imaginatively about how this technology can also help secure a space on the Internet for critical government and commercial applications."[114]

X. IS INTERNATIONAL LAW THE ANSWER?

One key issue to consider is that the United Charter only states if an armed attack is inflicted on a nation.[115] Whether this includes an attack on a nation's infrastructure is uncertain.[116] It is interesting to note that the notion of self-defense under Article 51 is broadly construed. If read strictly literally, the trigger for a state to exercise its right to self-defense is the "requirement of an armed attack." This means that an armed attack (in whatever form) must be carried out on a country

110. *Id.*

111. Noah Shachtman, *Cyber Command: We Don't Wanna Defend the Internet (We Just Might Have To),* WIRED (May 28, 2010), http://www.wired.com/dangerroom/2010/05/cyber-command-we-dont-wanna-defend-the- internet-but-we-just-might-have-to/.

112. *Id.*

113. *Id.*

114. *Id.*

115. *See* Jensen, *supra* note 12; Schaap, *supra* note 8; Hoisington, *supra* note 8; Barkham, *supra* note 8; Petras, *supra* note 8.

116. *See* Jensen, *supra* note 12; Schaap, *supra* note 8; Hoisington, *supra* note 8; Barkham, *supra* note 8; Petras, *supra* note 8.

before that country can use force without the U.N. Security Council's authorization.[117]

A. RETALIATION BY A NATION STATE TO CYBER-WARFARE

The ability of a nation state to respond to a cyber attack categorized as an act of war will depend on several varying factors such as impact and nature of the attack. What constitutes a use of force is crucial to the evaluation of whether the U.N. Charter is a viable mechanism for retaliation against an attack. Historically, the use of force prior to the U.N. Charter has been lengthy and the various international agreements have not always been effective in avoiding violence and war.[118] The United Nations followed the previous League of Nations, which limited a nation's ability to resort to war.[119] In accordance with Article 1 of the U.N. Charter, the main objective of the United Nations is to ensure and maintain international peace and security through collective measures and to block acts of aggression or breaches of peace.[120]

B. USE OF FORCE

The limitation on a nation's use of force is evidenced by Article 2 (4) which states:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the purposes of the United Nations.[121]

The object of this is twofold. First, a military action is authorized by the U.N. Security Council. Second, the entrenched international

---

117. *See* Jensen, *supra* note 12, at 219; Jurich, *supra* note 8; Solce, *supra* note 8.

118. *See* Jensen, *supra* note 12, at 219; Jurich, *supra* note 8; Solce, *supra* note 8; Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

119. *See* U.N. Charter preamble; *see also* Jensen, *supra* note 12, at 213; Petras, *supra* note 8; *see also* Myriam Dunn Cavelty, *Cyber-Terror- Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate*, 4 J. INFO. TECH. & POLITICS 1, 1 (2007); Joyner & Lotrionte, *supra* note 28; *see* Jurich, *supra* note 8; *see also* Solce, *supra* note 8, at 293-324; *see also* Aldrich, *supra* note 28, at 223-63; *see also* Schaap, *supra* note 8, at 122-74; *see also* Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8, at 57-113; *see also* Petras, *supra* note 8, at 1213-68.

120. U.N. Charter art. 1; *see* Jensen, *supra* note 12, at 214; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

121. *See* Jensen, *supra* note 12, at 214; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

legal principle of self-defense is maintained.[122] These are the two provisions which govern a nation's decision to use or threaten force under the *jus ad bellum* doctrine.[123] The U.N. Security Council's response to a breach of the U.N. Charter is provided in Article 39 where it "establishes a collective method of enforcement in response to a Charter violation by a breach of peace, threat to peace or an act of aggression."[124] It is the role of the U.N. Security Council to determine the existence of a threat, breach of peace, or act of aggression.[125]

Further, the U.N. Security Council will make any recommendations or decisions as to the course of action that must be taken by the aggrieved nation in accordance with both "Articles 41 and 42 to maintain or restore international peace and security."[126] Effectively, the role of the U.N. Security Council is to determine what action the aggrieved/attacked nation must take and the nature of the action as well as any preventative/remedial actions that are deemed appropriate.[127] However, an exception to this is provided in Article 51, which allows a nation the right to self-defense.[128] Article 51 provides that "nothing contained in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a Member of the United Nations until the U.N. Security Council has taken the measures necessary to maintain international peace and security."[129] There are two limitations on the doctrine of self-defense, namely "necessity" and "proportionality." The limitation of necessity is one where there is determined to be imminent danger of an armed attack, and proportionality is the "degree of force that is reasonable in terms of intensity, duration, magnitude, required to decisively counter the hostile

---

122. Jensen, *supra* note 12, at 214; *see* Jurich, *supra* note 8; Solce, *supra* note 8; *see* Aldrich, *supra* note 28, at 223-63.

123. Schaap, *supra* note 8, at 122-74; *see also* Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68; Jensen, *supra* note 12, at 214; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63.

124. *See* Jensen, *supra* note 12, at 207, 216; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

125. Jensen, *supra* note 12, at 214; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63.

126. Jensen, *supra* note 12, at 217; *see* Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

127. Jensen, *supra* note 12, at 217; *see also* Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

128. Jensen, *supra* note 12, at 217; *see also* Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

129. U.N. Charter art. 51; *see also* Jensen, *supra* note 12, at 218; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

part of the equation but no more than that."[130] If a nation acts on the basis of the self-defense provision, then the nation's action must be out of necessity and must be proportional to the threat against which it will be defending itself.[131] The doctrine of self-defense also incorporates the notion of anticipatory self-defense, which is used in certain cases where the doctrine of self-defense is not able to be properly considered. This notion of anticipatory self-defense was provided by the "Nineteenth Century U.S. Secretary of State Daniel Webster" who held the view that "when the necessity of self-defense is instant overwhelming and leaves no choice of means and no moment for deliberation, a nation may act pre-emptively to protect itself."[132] It is sufficient to assert that the doctrine of the use of force in self-defense is on the pathway to its demise due to the non-obligatory nature of international rules.[133] Commentators argue that Article 51 has no real practical force because "if there is no authoritative general prohibition of use of force it makes no sense to consider the breadth of a possible exception."[134]

XI. RETALIATION BY A GOVERNMENT TO CYBER-TERRORISM

A. IS CNA A USE OF FORCE?

Whether or not a computer network attack (CNA) constitutes a "use of force" is considered necessary in order to determine the legal response of a nation in accordance with international law.[135] Further, there are various levels of CNAs which can affect a nation's infrastructure. For example, a CNA will not always qualify as an armed attack because of the various degrees of what can constitute such a CNA. It can be anything from "crashing" a website to preventing emergency services and harming civilians. One commentator asserts:

---

130. *See generally* Richard Grunawalt, *The JCS Standing Rules of Engagement: A Judges Advocate's Primer*, 42 A.F. L. REV. 245 (1997); Jensen, *supra* note 12, at 218; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

131. Jensen, *supra* note 12, at 218; *see* Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; *see also* Petras, *supra* note 8, at 1213-68.

132. *See* Jensen, *supra* note 12, at 218; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

133. *See* Michael J. Glennon, *The Fog of Law: Self Defense Inherence and Incoherence in Article 51 of The United Nations Charter*, 25 HARV. J.L & PUBLIC POL'Y 539, 539 (2002); *see also* MICHAEL J. GLENNON, LIMITS OF LAW, PREROGATORIES OF POWER: INTERVENTIONISM AFTER KOSOVO (2001).

134. *See* Glennon, *The Fog of Law*, *supra* note 133; Jensen, *supra* note 12, at 217; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

> A CNA challenges the prevailing paradigm for its consequences cannot easily be placed in a particular area along the community values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g. shutting down an academic network temporarily) to physical destruction (e.g. as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g. shutting down power to a hospital with no back-up generators. It can affect economic, social, mental, and physical well-being either directly or indirectly, and its potential scope grows almost daily being capable of targeting everything from individual persons or objects to entire societies.[136]

One criticism of this statement is that it is not "reasonable to assume that the CNA will meet the level of a use of force pursuant to the U.N. Charter."[137] Similarly, it is not reasonable to think that because the CNA may not destroy the object of attack (in a physical sense) it "can never amount to a use of force or an armed attack."[138] In this respect, there must be an allowance for the different level of CNA to "fit into all three categories. This problem is complicated by the few known examples of CNAs which make it difficult to assess what States will ultimately consider appropriate when dealing with CNAs and the use of force."[139]

Two main arguments, which relate to whether the level of CNA will amount to a use of force under the U.N. Charter, are as follows:

1. threats to use force may rise to the level of an unlawful use of force in violation of Article 2(4) but may not trigger a nation's Article 51 right to anticipatory self-defense;[140] and

---

136. *See* Jensen, *supra* note 12, at 222; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

137. *See also* Jensen, *supra* note 12, at 207, 216; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

138. *See* Jensen, *supra* note 12, at 216, 222; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

139. *See* Jensen, *supra* note 12, at 207, 216; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

140. Jensen, *supra* note 12, at 223; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

2. a threat to use force that is short of actual use demonstrates hostile intent and triggers a nation's right to anticipatory self defense.[141]

Another argument is that "Article 2(4) prohibition on the use of force also covers 'physical force of a non-military nature' committed by any State agency and that such non-military actions may produce the effects of an armed attack prompting the right of self defense laid down by Article 51 of the U.N. Charter."[142] This is applicable by analogy to CNA's due to the nature of a computer network. For example, a computer network attack (which has been carried out by another State actor) that "intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self defense under Article 51 of the U.N. Charter."[143] There are many analogous examples for this such as the unlawful (and unauthorized) penetration of a country's airspace (e.g., Turkey's invasion of Greece's airspace by flying over Greek islands). Commentators have argued that mere penetration of a nation's cyberspace is not a use of force despite it possibly violating domestic law.

Some commentators argue that it is the consequences of the attack rather than the attack or the intentions of the attacker that should be more in focus.[144] Further, they argue that a more restrictive reading of the notion of self-defense should be taken. There are exceptions to this however, which are cases where "an attacker intends to cause injury to human beings or cause physical damage to objects."[145] These cases would fulfil the requirement of use of force under the U.N. Charter, although when the element of intention is missing, the consequences of the attack should be considered.[146]

---

141. Jensen, *supra* note 12, at 223.

142. *Id.* at 216, 223; *see* Joyner & Lotrionte, *supra* note 28; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

143. *See* Jensen, *supra* note 12, at 223; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

144. Jensen, *supra* note 12, at 223; *see also* Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

145. Jensen, *supra* note 12, at 222; *see also* Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

146. *See* Jensen, *supra* note 12, at 223; Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

Essentially, even if the CNA did not amount to an armed attack it would still fall within the use of force ambit, if the effects of the attack are equivalent to those "effects that would result from a similar attack with armed force."[147] One commentator suggests that anticipatory self-defense must have three elements present:

1. The CNA is part of an overall operation culminating in armed attack;
2. The CNA is an irrevocable step in an imminent (near term) and probably unavoidable attack; and
3. The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.[148]

It has been suggested in broad terms that computer networks are vital to national security. In 1996, U.S. President Clinton signed Executive Order 13,010, which stated:

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue) and continuity of government.[149]

At that time, the Executive Order stated the vulnerabilities of critical infrastructures. It provided that "threats to these critical infrastructures fall into two categories, physical threats to tangible property (physical threats) and threats of electronic, radio-frequency or computer based attacks on the information or communication components that control critical infrastructures (cyber threats)."[150]

It is noted that the Order is silent as to what the response to an attack should be; however, in October 2001 President George W Bush, reaffirmed Clinton's view in Executive Order 13,231 entitled "Critical Infrastructure protection in the Information Age." In that order, it was stated that "protection of critical infrastructure systems is essential to

---

147. *See* Jensen, *supra* note 12, at 223; Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

148. Jensen, *supra* note 12, at 223; *see also* Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

149. Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (1996), *reprinted as amended in* 42 U.S.C. § 5195 (2000) [hereinafter Exec. Order 13,010] (defining which systems are sensitive and vital)); *see also* Jensen, *supra* note 12, at 226; Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

150. Exec. Order No 13,010; *see also* Jensen, *supra* note 12, at 226; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28.

telecommunications, energy, financial services, manufacturing water, transportation health care, and emergency service sectors."[151] Further Bush's commitment to act when U.S. infrastructures are threatened was cemented in Executive Order 13,231 which stated:

> It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States and to ensure that any disruptions that occur are infrequent, of minimal duration, manageable, and cause the least damage possible.[152]

This Order established the National Infrastructure Advisory Council (NIAC), which provides the President with advice on the security information systems for critical infrastructure supporting other sectors of the economy, such as banking and finance, transportation, energy, manufacturing, and emergency government services.[153] Presently, there are no explicit guidelines as to how to respond to cyber attacks.

XII. RETALIATION – CAN IT BE JUSTIFIED?

The form of response to a cyber attack will differ depending on the nature of the attack, the target of the attack, and the impact of the attack, e.g. actual disruption of services or damage to infrastructure or denial of service against that infrastructure. Australian legislation does not clearly allow a "counterattack" or strike-back action against a private computer or another nation's infrastructure. A retaliatory attack on a private electronic system in response to a criminal or terrorist act would need to be justified as either self-defense or be allowed under legislation. Justification of a retaliatory attack by one nation against the infrastructure of another relies upon international laws and conventions. The U.N. Convention on the Use of Force is one possible instrument that could potentially allow for a nation to "strike back" against a cyber attack. There are no known instances where the U.N. Convention has been used to counterattack another nation state. There are conflicting views in relation as to whether a computer network attack would be

---

151. *See* Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

152. Exec. Order No. 13231, 66 Fed. Reg. 53063 (Oct. 18, 2001), *available at* http://www.ara.gov/fedreg/eo2001b.html; *see also* Jensen, *supra* note 12, at 227; Joyner & Lotrionte, *supra* note 28; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

153. Exec. Order No. 13231, 66 Fed. Reg. 53069 (Oct. 18 2001), *available at* http://www.ara.gov/fedreg/eo2001b.html; *see also* Jensen, *supra* note 12, at 227; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

classified as an act of war (as the term is construed by the wording of the U.N. Convention). While the U.N. Convention may potentially provide the means for a nation to defend itself, there are significant questions arising in relation to whether "cyber attacks" are comparable to "armed attacks" as referred to by the Convention.

A. RESPONDING TO CNA IN ANTICIPATORY SELF-DEFENSE

There are various options for responding to CNA attacks; however, this Article limits the discussion to only CNA attacks in relation to a use of force.[154] Computer Network Defense (CND) offers a working basis for the type of defense for an attack. There are two types of CND to protect computers and networks from a CAN: passive measures and active measures.[155] Passive measures are encryption, firewalls, and automatic detection. Active measures include rejoinder or hack back features.[156]

B. ATTRIBUTION OF THE ATTACK

Attribution relates to whether the attacked country can respond lawfully without having knowledge of the identity of the attacker. Trying to ascertain the true identity and location of any attacker can be time consuming and difficult to determine. In particular, indisputable knowledge of the location of the attacker and the reliable assessment of damage that has been caused from an attack are difficult matters.[157] This can have an adversary effect on the attacked nation if it has to wait to identify the attacker and his location, as well as to strategize on what course of action it must take.[158]

---

154. Jensen, *supra* note 12, at 230; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

155. S*ee also* Jensen, *supra* note 12, at 230; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

156. Jensen, *supra* note 12, at 231; *see* Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

157. *See* Jensen, *supra* note 12, at 232; *see also* Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

158. *See* Jensen, *supra* note 12, at 233; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

C. CHARACTERIZATION OF THE ATTACK

There is difficulty in ascertaining the nature of the attack. Specifically, characterizing the nature of an attack in a way whereby the attacker's intention will be deemed hostile.[159] One of the difficulties is that CNA does not fall under the traditional and conventional type of kinetic weapons.[160] The significance of this is that once a hacker has broken through all of the defenses of a computer, it can realize his intentions instantaneously.[161] This is of particular concern as information systems may be infected with viruses or flooded with requests, resulting in a denial of service attack. These may prevent the business or government department from continuing to provide its services, as demonstrated by the example of attacks on Estonia and Georgia. Moreover, such penetrations of computer systems and networks may lay dormant for periods awaiting automated or remote activation.

XIII. CONCLUSION

Interestingly, had the attacks been on critical information infrastructures, such as telecommunications and power so as to cause extensive physical damage, then perhaps the strike and counter attack options may be viable. However, in the example of Georgia's counter attack, the damage caused indicated the limited impact that a counter attack could have on the attacking nation. In a cyber attack, it is simpler to cause the same damage as what a physical attack would have if the attacking nation targeted critical information systems as the majority of nations and societies are increasingly dependent and reliant on information systems and computer networks. The question remains as to whether the existing legal frameworks provide adequate response measures for cyber attacks; more significantly, whether the deemed responses are adequate to protect a nation through the U.N. Convention.

---

159. *See also* Jensen, *supra* note 12, at 235; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74;Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

160. *See* Jensen, *supra* note 12, at 231; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.

161. *See* Jensen, *supra* note 12, at 231; Joyner & Lotrionte, *supra* note 28; Jurich, *supra* note 8; Solce, *supra* note 8; *see also* Aldrich, *supra* note 28, at 223-63; Schaap, *supra* note 8, at 122-74; Hoisington, *supra* note 8, at 439-54; Barkham, *supra* note 8; Petras, *supra* note 8, at 1213-68.