Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

International Cybercrime Treaty: Looking Beyond Ratification

The Cybercrime Treaty is vital if the growing threat of global cybercrime is to be met. It is a world-wide approach to incident handling. It is hard to determine whether amendments to the Treaty in response to the demands of citizens or changes to various governments' approach to cybercrime itself will enable the Treaty to succeed. The Cybercrime Treaty could also be expanded to include other nations or set the groundwork for an even more encompassing international treaty. If the Cybercrime Treaty turns out to be inca...

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2007, Author retains full rights.

International Cybercrime Treaty: Looking Beyond Ratification

GCIH Gold Certification

Author: Dan Robel, robelda@saic.com

Adviser: Joey Niem

Accepted: August 15th 2006

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Outline

1. Introduction To Global Incident Handling..... 4

A. Classic Case.....4

B. Definition of Global Incident.....5

2. Background.....7

A. Origins of the Treaty.....7

B. Primary Premise and Key Components 9

3. Issues with Cybercrime Treaty..... 11

A. Promotes Knowledge and International Cooperation.....12

B. Human Rights and Civil Liberties 18

C. Deals with Intellectual Property.....20

D. Restricts Hacking Tools.....22

E. Borderless Nature of Internet..... 25

4. Focus: Possible Effectiveness And Impact Of Treaty 26

A. Comparison of Non-Treaty versus Treaty Nations..... 27

B. United States Ratification Serving as a Precedent.....32

C. Issues as They Stand.....34

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5. Illustrative Scenarios 35

A. Past Example of How the Treaty Would Not Have Affected 35

B. Hypothetical Example of Circumvention 37

B. Past Example Where International Cooperation Succeeded 41

6. Conclusion 42

7. References 45

© SANS Institute 2007, Author retains full rights

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. INTRODUCTION TO GLOBAL INCIDENT HANDLING

A. Classic Case

Imagine military sites are being attacked on the Internet and the source of the attacks can be traced to a major academic university within the country. Now imagine that the root cause is not a bored programming student, but a nefarious plot from a foreign intelligence agency willing to pay a group of computer hackers to penetrate into the military computers of a rival nation. The hacking group manages to gain access to a university undetected and from this quiet world of academia, launches several attacks against sensitive military sites. Eventually a member of the faculty of the university indirectly discovers this malicious activity. Through a breadcrumb trail of clues, it results in an international investigation coordinated between the law enforcement agencies of the victim nation and the nation where the hacking group resides, and the perpetrators are brought to justice. To some this scenario would sound like prime material for a good fiction novel. To others, this scenario will sound very familiar. This very situation has been referenced in several reports and lectures on computer hacking, and is the story portrayed in Cliff Stoll's Cuckoo's Egg, which is based on the author's real life experiences.

Many people, especially those involved in information security, are familiar with this story. The author discovered a 75-cent accounting error while working in the Lawrence Berkeley Lab, which eventually resulted in the discovery of unauthorized network access and used by an individual going by the moniker of "Hunter." Basing from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Berkley's network, this hacker launched several attacks against various military sites. Coordinating with law enforcement and federal agencies, the author managed to trace these attacks to Hanover, Germany. With the assistance of German law enforcement, the hackers were brought to justice.[1]

The more detailed version is likely less known or remembered. The KGB of what was the then Soviet Union was paying the West German hacking group known as the Chaos Computer Club to gather data from the United States. This group was being paid to penetrate into United States military computers under an intelligence effort known as Project Equalizer. It is members of this hacking group that managed to break into Lawrence Berkley Labs and utilize its network resources to pursue their agenda. It is this group that would later become the focus of Cliff Stoll's hunt.[2]

While sensationalized in Cliff Stoll's novel, such a situation is not a freak occurrence, or unlikely to happen again. It is in point of fact a classic example of the global nature of incident handling in today's world. One may ask, 'what is a global incident?'

B. Definition of Global Incident

---

[1] Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Pocket Books, 1990.

[2] Sarkar, A. (2004, August 24). The Cuckoo's Egg by Clifford Stoll. Retrieved January 14, 2007 from http://www.cs.sfu.ca/~anoop/weblog/archives/000052.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The term "incident" refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event (e.g. Unauthorized use of another user's account, Unauthorized use of system privileges, Execution of malicious code that destroys data). An incident implies harm or the attempt to harm.[3] For the purposes of this paper, a "global incident" can be defined as an incident involving the computers, network, or assets of more than one nation-state. Such a situation is aptly noted by Dr. Vladmir Golubev, the Director of the Computer Crime Research Center (CCRC), "Anonymity and absence of frontiers makes the Internet an efficient weapon in hands of criminals. In the virtual space criminals usually act from sites in other countries."[4] Three primary situations can be defined as a global incident. The first is an incident where the country of origin from whence an attack or malicious activity originates differs from the country where the incident takes place. The next is an incident where all activity happens within one nation's physical borders, but assets (whether computers, data, etc) are owned by another nation. The last is where multiple nations are affected including the nation where the attack originated. One may think that attacks of this nature are infrequent and would not make the news. However, statistics would indicate that as recent as late 2005, the money accrued through

---

[3] SANS. *Incident Handling Step-by-Step and Computer Crime Investigation*. (The Sans Institute, 2006), 6-7.

[4] Golubev, V. (2004, June 16). *International Cooperation in Fighting Transnational Computer Crime*. Retrieved January 14, 2007 from http://www.crime_research.org/articles/431/.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

cybercrime had surpassed even that made from the global drug trade, reaching a startling 105 billion dollars.[5] Larry McNiven, a US advisor on cybercrime, states "Cybercrime is moving at such a high speed that law enforcement cannot catch up with it."

Given the growing threat of Global cybercrime and the political and legal difficulties in coordinating law enforcement across international lines, several attempts have been made to facilitate cooperation between nations. One recent and ambitious undertaking is the Council of Europe's Convention on Cybercrime (hereinafter referred to as the Cybercrime Treaty or the Treaty).

2. BACKGROUND

A. Origins of Treaty

The Council of Europe refers to the union of 41 nations of Europe, which was established in May of 1949 in order to facilitate social and economic growth and foster unity among its members. It is headquartered in Strasbourg, France.[6] The Cybercrime Treaty has been the subject of much consideration by the European Union since as early as 1997. The goal of this treaty was viewed as an attempt to "harmonize

---

[5] Leydon, J. (2005, November 29). *Cybercrime 'more lucrative' than drugs*. http://www.channelregister.co.uk/2005/11/29/cybercrime/.

[6] The Maudit Group. (n.d.). *Glossary and Acronyms - International Business - Con to D*. Retrieved January 14, 2007 from http://www.rmauduit.com/glossary-con.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

laws against malicious hacking, virus writing, fraud and child pornography on the net. It also aims to ensure that police forces in separate countries gather the same standard of evidence to help track and catch criminals across borders."[7] Since cybercrime often transcends a nation's borders in being committed, the measures to combat it must also be of an international nature.

The Treaty itself, after going through a number of draft forms including a final draft on May 23, 2001, was introduced on November 23, 2001 in Budapest. The treaty from that point forward was open to be signed by any nation involved, and subsequently ratified. January 7, 2004, the Treaty went into force with 5 nations ratifying the Treaty and fulfilling the requirement for minimum number of signatories. On June 17, 2004, the United States' Senate's Committee on Foreign Relations held a hearing to discuss ratification of the treaty.[8] On August 4, 2006, the U.S. Senate finally ratified the treaty.[9]

---

[7] BBC News. (2000, December 18). *Cybercrime Treaty Condemned*. Retrieved January 21, 2007 from http://news.bbc.co.uk/1/hi/sci/tech/1072580.stm.

[8] Lugar, R. (2004, June 17). *Committee on Foreign Relations United States Senate Hearing*. Retrieved January 14, 2007 from http://www.senate.gov/~foreign/hearings/2004/hrg040617a.html.

[9] McCullagh, D & Broache, A. (2006, August 4). *Senate Ratifies Controversial Cybecrime Treaty*. Retrieved January 14, 2007 from http://news.com.com/Senate+ratifies+controversial+cybercrime+treaty/2100-7348_3-6102354.html. CNET.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

B. Primary Premise and Key Components

The Treaty itself accomplishes three key goals. The first goal is the establishment of a specific list of domestic criminal offenses and conduct that are prohibited by the treaty. The second goal is to adopt a set of procedural tools and powers to properly and effectively investigate crimes. The last goal is to establish strong mechanisms for fostering international cooperation.[10]

Articles two through eleven of the Treaty accomplish the first goal of prohibiting specific types of conduct.[11] Each nation that signs the treaty is expected to outline certain mandatory criminal offenses and conduct and the related sanctions for crimes committed within that nation, territories in their possession, on the nation's ships and aircraft, and by their citizens when they are abroad as foreign nationals. The offenses are broken down into four areas of crime, which are fraud and forgery, child pornography, copyright infringement (intellectual property), and system interferences, which affect network integrity and availability (covering many aspects of hacking). Due to objections by the United States, an additional

---

[10] Senate Foreign Relations Committee. (2004, June 17). *Statement of Bruce Swartz; Deputy Assistant Attorney General; Criminal Division; Multilateral Law Enforcement Treaties*. Retrieved January 14, 2007 from http://foreign.senate.gov/testimony/2004/SwartzTestimony040617.pdf.

[11] Global Lawful Interception Forum. (n.d.) *Eight Reasons the US Should Ratify the Cybercrime Treaty*. Retrieved January 14, 2007 from http://www.gliif.org/RafityNow/reasons.htm.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

provision prohibiting racist acts (e.g. distributing racist materials) on the Internet was kept separate of the treaty itself to be approved as its own protocol. The United States has not signed this protocol on the grounds it would violate freedom of speech.[12]

Articles sixteen through twenty-two of the Treaty accomplishes the second goal of ensuring the establishment of a national legal process for each country, including human rights safeguards, legal procedures, and the tools and procedures that will be used for criminal investigation.[13] Each nation must create specialized procedures for detecting, investigating, and prosecuting computer crimes and collecting any electronic evidence of the crime. Particularly of note, this provision includes the preservation of computer stored data and communications, system search and seizure, and real-time "wire-tapping" on the network.[14] The chief reasoning behind this section of the treaty is the fact that cybercrime, and electronic communications in general, is generally fast, efficient, and hard to isolate. In order to obtain electronic evidence in a timely matter, the proper procedural tools and powers are needed to expedite matters so that the appropriate

---

[12] Archik, K. (2004, July 22). CRS Report for Congress. Cybercrime: The Council of Europe Convention. Retrieved January 21, 2007 from http://fpc.state.gov/documents/organization/36076.pdf.

[13] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty.

[14] Archik, K. (2004, July 22). CRS Report for Congress. Cybercrime: The Council of Europe Convention.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

evidence can be secured.[15]

Articles twenty-three through thirty-five outline the third goal of creating an environment for international cooperation. It includes the areas where cooperation in cybercrime investigation is appropriate and also addresses the matters of confidentiality and the conditions of use.[16] This last major provision establishes guidelines for extradition, collection of computer-based evidence in another country, and a 24x7 network that can provide immediate assistance in international investigations.[17]

3. ISSUES WITH CYBERCRIME TREATY

The Treaty, while simple in its fundamental goal, is far-sweeping in the areas it attempts to address and touch upon. Given the myriad of issues arising from the Treaty, much controversy has sprung up over various points. It is not the purpose of this study to debate one side over another on any issue. This study also does not represent a

---

[15] Senate Foreign Relations Committee. (2004, June 17). Statement of Bruce Swartz; Deputy Assistant Attorney General; Criminal Division; Multilateral Law Enforcement Treaties. Retrieved January 14, 2007 from http://foreign.senate.gov/testimony/2004/SwartzTestimony040617.pdf.

[16] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty.

[17] Archik, K. (2004, July 22). CRS Report for Congress. Cybercrime: The Council of Europe Convention.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

comprehensive examination of all the possible issues that may arise due to ratification of the Treaty. However, it is deemed important to understand many of the underlying issues and possible effects of the treaty going into effect, to determine whether the effectiveness of the treaty and its argued strong points justify the possible risks and controversial issues that may become a reality in the future.

A. Promotes Knowledge and International Cooperation

I) Chief Strong Points

Some of the chief heralded strengths of the Treaty lie in its built-in mechanisms to help avoid conflict and friction between various nations, and their different legal processes. The Justice Department stated it as being able to eliminate "procedural and jurisdictional obstacles that can delay or endanger international investigations."[18] The Treaty from the outset outlines what areas and provisions will have a different handling of the procedural or substantive legal processes. More importantly current issues that were known to cause conflicts among nations were addressed. This is a tremendous stride given a common lack of knowledge of cybercrime laws as it pertains beyond the United States' borders.

To illustrate this point, a survey was conducted in 2004 by CSO

---

[18] McCullagh, Declan. *President Bush has asked the US Senate to ratify the first international cybercrime treaty. Retrieved January 14, 2007 from http://news.zdnet.com/2100-1099_22-5108854.html.*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

magazine in conjunction with the Secret Service and Carnegie Mellon University Software Engineering Institute CERT CC. The survey interviewed five hundred individuals knowledgeable of cybercrime. Two-thirds of those surveyed were in security or IT management-related positions (thirty-two and thirty-four percent respectively). Twelve percent hold jobs as either law enforcement or prosecutor, and the rest are corporate managers outside the IT field. The survey has revealed that while only thirteen to fourteen percent of those surveyed were ignorant of local or national cybercrime law, a significant forty-two percent were unaware of internationals laws that governed cybercrime. The Treaty would harmonize international cybercrime laws and create greater awareness.[19]

The Treaty also allows for any nation when signing or ratifying to state declarations or reservations towards any of the obligations tied to the provisions of the Treaty. The United States has already exercised this right and has six reservations and four declarations to ensure that the nation's civil liberties and the integrity of its legal process are maintained.[20] In addition, the United States did not need to create any new laws in order to be eligible to be part of the Treaty. Such a distinction may be one of the reasons that the treaty

---

[19] Cert Coordination Center. (2004). 2004 eCrimeWatch Survey Summary of Findings. Retrieved January 21, 2007 from http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf.

[20] Powell, C. (2003, September 11). Letter of Submittal. Retrieved June 30, 2004 from http://www.usdoj.gov/criminal/cybercrime/senateMemo.pdf.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

was ratified. Given the concerns over the powers given by this Treaty, one of the strongest selling points is that it reflects a much of existing United States Federal and State laws. As stated by Stansell-Gamm, the Justice Department's Computer Crime and Intellectual Property Section Chief, "If countries go overboard writing laws to implement the treaty, it won't be because of the treaty itself."[21] US negotiators and representatives have vigorously worked to eliminate any controversial provisions or protocols that are not in keeping with US law and procedure.[22]

Furthermore, no new law or legislation will need to be implemented. In a letter from Colin Powell representing the State Department to the Presidents' office, it is stated that the Treaty "would not require implementing legislation for the United States… existing US federal law, coupled with six reservations and four declarations, would be adequate to satisfy the Convention's requirements for legislation. All of these reservations and declarations are envisaged by the Convention itself. Since other provisions contained in the Convention are self-executing (e.g., articles relating to extradition and mutual assistance), they would not

---

[21] Roger, W. (2001, June 26). *Cybercrime treaty raises privacy and commerce questions*. Retrieved January 14, 2007 from http://techrepublic.com.com/5100-6298_11-1040577.html.

[22] Archik, K. (2004, July 22). *CRS Report for Congress. Cybercrime: The Council of Europe Convention*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

require implementing legislation either."[23] The reservations and declarations themselves help apply additional threshold requirements to sensitive offenses under the Treaty and ensure that Treaty obligations will be conducted in a manner consistent with existing federal legislation.[24]

The types of criminal offenses addressed, are also already existent under United States law. This provision in the Treaty is beneficial to the United States, as it requires other countries that hackers can be operating from to have similar laws, so that the hacker cannot hide behind that nation's laws. It is hoped that this will serve as a further deterrent to the criminal, knowing that United States' laws extend elsewhere. The procedural tools given under the treaty also mirror United States law and is more an assurance that if the data trail leads to another country, that there would be greater chance of successfully tracing the hacker back to the source, instead of letting the trail die once it left national borders.[25]

II) Lack of dual criminality

---

[23] Powell, C. (2003, September 11). Letter of Submittal.

[24] Senate Foreign Relations Committee. (2004, June 17). *Statement of Bruce Swartz; Deputy Assistant Attorney General; Criminal Division; Multilateral Law Enforcement Treaties*.

[25] Senate Foreign Relations Committee. (2004, June 17). Statement of Bruce Swartz; Deputy Assistant Attorney General; Criminal Division; Multilateral Law Enforcement Treaties.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

However, The Treaty's lack of a need to change most laws within countries and its goal of facilitating and expediting cooperation among nations has another side to it. There is a concern tied to Article 25 of the Treaty. The article holds that "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense."[26] This means that the United States will be called on to assist other countries in enforcing their laws.

The core problem, as some see it, is that the Treaty lacks a "dual criminality" provision. A dual criminality provision would require that for an offense to be considered a crime under the Treaty, it would have to be a crime in both the nation it was committed in, and in the nation whose assistance is being lent. The Treaty currently requires that it only be a crime in the country that the action is committed. This may result in the US conducting an internal investigation on US soil on behalf of another nation for an action that is not a crime according to US law.[27] The reverse case also would raise issues in

---

[26] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*. Retrieved September 1, 2007 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[27] The American Civil Liberties Union. (n.d.) *8 Reasons for US to Reject the International Cyber Crime Treaty*. Retrieved January 21, 2007 from http://www.totse.com/en/law/justice_for_all/165280.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the pursuit of Cybercrime and cause international friction.

Barry Steinhardt of the ACLU pithily portrayed one view of the situation. "This is a bad treaty that not only threatens core civil liberties, but will obligate the United States to use extraordinary powers to do the dirty work of other nations."[28] There is even an argument by the Global Internet Liberty Campaign (a collection of civil society organizations from around the world) that the Treaty itself goes against certain principles of human rights and privacy as laid out by the European Convention on human rights and the European Court of Human Rights.[29]

The Treaty has a built-in provision, which states that when another country asks for assistance, "The requested Party may… refuse assistance if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence."[30] This is intended to help avoid problems as previously described where the United States' resources can be used for political ends by another nation or to cowl political dissent. Unfortunately, there is no exemption for political offenses in dealing with real-time

---

[28] Rizvi, H. (2004, January 21). *Bush's Plan to Increase Internet Surveillance*. http://www.alternet.org/rights/17633.

[29] Global Internet Liberty Campaign. (2000, October 18). Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime.

[30] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

data monitoring.[31] Moreover, some nations treat what the United States would consider political crimes as civil infractions. This gives the political exemption provision limited power. A good example of this would be the ratified nation of Romania. In Romania, libel against a public official carries a criminal penalty up to three years. There are also penalties for spreading false information aimed at attacking national security. These type of laws are civil not political and the United States could be called to use its resources. There is also the complaint that the Treaty outlines that "central authorities will communicate with each other directly,"[32] creating a situation where law enforcement can act directly in mutual assistance without judicial oversight or approval, further exacerbating this problem.[33] These issues may be cause for concern given the ratification of the Treaty.

B. Human Rights and Civil Liberties

I) Preamble Addresses Human Rights and Privacy

Another chief strongpoint of the Treaty is that it specifically

---

[31] The American Civil Liberties Union. (n.d.) 8 Reasons for US to Reject the International Cyber Crime Treaty.

[32] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*.

[33] A Global Internet Liberty Campaign. (2000, October 18). Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

addresses the concern of human rights and privacy and goes so far as address it in the preamble of the document.

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights, as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the protection of personal data, as conferred e.g. by the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data…[34]

II) Can be abused to reduce rights

A related issue is the fact that privacy and human rights are addressed minimally in the Treaty itself. In fact, other than the preamble, there is no mention of or provision for citizen's privacy.[35]

---

[34] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*.

[35] Legal Affairs Treaty Office. (2001, November 23). Council of Europe

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

One privacy expert reporting to the Global Internet Liberty Campaign surmised that the Treaty would lead to "fundamental restrictions on privacy, anonymity, and encryption."[36] The main problem seems to lie in the fact that the Treaty in its wording attempts to transpose its guidelines into the existing domestic laws of ratifying countries. In the United States, this could very well work given the solid foundation of laws set out by precedent, federal law, and the United States Constitution. However, by trying to work with other nations' existing domestic laws, the process may result in "drastically different pre-existing privacy and human rights protections."[37] The lack of specific guidelines within the Treaty may result in conflicts of law during times where the United States' assistance is requested.

C. Deals with Intellectual Property

I) Protects intellectual property

Another aspect of the Treaty that is held up as a strong point is the intellectual property enforcement provision (addressed in Article

---

Convention on Cybercrim

[36] Global Internet Liberty Campaign. (2000, October 18). *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*.

[37] Electronic Privacy Information Center. (2004, June 17). *Letter to Richard G. Lugar and Joseph R. Biden, Jr*. Retrieved January 14, 2007 from http://www.epic.org/privacy/intl/senateletter-061704.pdf. Privacy Information Center.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

10 of the Treaty). Software, motion picture, and recording companies have spoken out in support of the Treaty. As a lot of piracy is done outside the United States, establishing a basis to enforce copyright in other countries will go a long way to counteracting this problem.[38] By some estimates, counterfeiting now accounts for 5% to 7% of world trade. Some now contend that counterfeiting and piracy are as profitable as trading in illegal narcotics and a lot less risky. Provisions against the abuse of intellectual property are a central concern for the United States. According to the 2006 Economic Report to the President, intellectual property accounts for more than one-third of the value of all US corporations, an amount equal to almost half of the United States' Gross Domestic Profit.[39] The Treaty does not overstep its bounds in enforcing intellectual property, as it only deals with countries that have already assumed property protection responsibilities due to other longstanding treaties in place.[40] These countries are obligated to enforce these protections when there are "willful infringements… committed by means of a computer system and on a commercial scale." However some organizations such as the Software

---

[38] Roger, W. (2001, June 26). *Cybercrime treaty raises privacy and commerce questions*.

[39] Watson, D. (2006, June 7). IPR Issues and Dangers of Counterfeited Goods Imported into the U.S. Retrieved January 14, 2007 from http://www.uscc.gov/hearings/2006hearings/written_testimonies/06_06_07wrts/06_06_7_8_watson_diane.php.

[40] Global Lawful Interception Forum. (n.d.) Eight Reasons the US Should Ratify the Cybercrime Treaty.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Business Alliance believe that the Treaty does not do enough. They have stated that they "welcome Article 10 of the draft Convention, which requires signatories to criminalize the reproduction and distribution of copyright protected material on-line. At present, however, the Article is too narrow in scope…"[41]

II) Can be over interpreted

The ACLU has raised a concern over Article 10.1 and the lack of a "fair use" clause in dealing with copyright within the Treaty. It criminalizes copyright infringement and makes it an extraditable offense.[42] The concern is that a misunderstanding of copyright by another country may cause an issue that in this country could be considered a "fair use" case of copying of materials. This lack of consideration for fair use is argued as a possible danger in our relations with other nation's and their differing copyright laws.

D. Restricts Hacking Tools

I) Helps prevent abuse

To help improve the fight against cybercrime, there will also be a

---

[41] Business Software Alliance. *BSA Comments on Convention*. (2000, September 8). Retrieved June 25, 2004 from http://global.bsa.org/security/resources/2000-09-08/06.doc.

[42] The American Civil Liberties Union. (n.d.) *8 Reasons for US to Reject the International Cyber Crime Treaty*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

criminalization of hacking tools including possession, creation, and distribution, where the conduct is "i) intentional, (ii) "without right", and (iii) done with the intent to commit an offense of the type described in Articles 2-5 of the Convention."[43] Supporters of the Treaty point out that the Article only criminalizes possession of such tools when the conduct is "i) intentional, (ii) "without right", and (iii) done with the intent to commit an offense of the type described in Articles 2-5 of the Convention." Paragraph 2 of article 6 also expounds that legitimate scientific research and system security practices are not criminal under this Article.[44] The clause mainly rests upon the criminal intent. This will help prevent the spreading of tools that can be used for cyber-terrorism and information warfare, and help make the job of reducing cybercrime easier.

II) Restricts innovation, research, and possibly proof of concept

Again, this 'strength' of the Treaty also is said to have a flip side. While it appears contradictory to the previously argued strongpoint of the treaty, it is said that Article 6 of the Treaty is a cause for concern, due to the fact that it makes production,

---

[43] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*.

[44] The Department of Justice. (2003, November 10). *Frequently Asked Questions and Answers: Council of Europe Convention on Cybercrime*. Retrieved January 14, 2007 from http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA11.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

distribution and use of "hacking tools" and exploit code illegal.[45] Some feel it is overly broad and actually criminalizes the tools themselves and not the behavior.[46] This problem as stated by some of the provision's opponents is that the provision is not specific enough and may discourage the creation of useful new security tools. Some data protection officials have theorized that "proposed treaty may inadvertently result in criminalizing techniques and software commonly used to make computer systems resistant to attack" and that it "would adversely impact security practitioners, researchers, and educators."[47] The problem of those against appears to be with the "criminal intent stipulation" previously mentioned due to the fact that it may arguable what is considered legitimate creation and distribution. In 2001, Eeye Digital Security released a proof of concept code for an exploit against IIS that was later used for a version of the Code Red Worm. Also, proof-of-concept code is used regularly by some for testing system security for existing vulnerabilities. If the creation of a workable exploit is used later for criminal purposes, some worry that the initial creation or later distribution could be viewed as illegal

---

[45] Meinel, C. (2004). *International Convention on Cybercrime Could Chill Computer Security Research*. Security & Privacy, Vol. 2 (No. 4), 28-32.

[46] The American Civil Liberties Union. (n.d.) *8 Reasons for US to Reject the International Cyber Crime Treaty*.

[47] Global Internet Liberty Campaign. (2000, October 18). *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

or punishable.[48] Further, Article 6.1 criminalizes distribution "without right", which is also a vague term that can cause legal difficulty for creators of security tools and proof of concept exploits.[49] This is another instance where the language of the Treaty appears to raise concerns of possible legal ramifications in the future. This is especially true due to the fact that citizens may be dealing with foreign governments, and they may interpret this Treaty and its provisions differently than their counterparts in the United States government.

E. Borderless Nature of Cybercrime

I) International cooperation and easier assistance

The key focus of this study and the main argument is that the Cybercrime Treaty will help address the issue of trans-border cybercrime. A nation's borders in general, do not restrict cybercrime, due to the nature of the Internet.[50] As mentioned earlier, a person behind a computer can just as easily connect to a computer in another country across the ocean as a computer within the same general region.

---

[48] Meinel, C. (2004). *International Convention on Cybercrime Could Chill Computer Security Research*.

[49] The American Civil Liberties Union. (n.d.) *8 Reasons for US to Reject the International Cyber Crime Treaty*.

[50] Global Lawful Interception Forum. (n.d.) *Eight Reasons the US Should Ratify the Cybercrime Treaty*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

This means that the United States has great difficulty in addressing crime committed against the United States by an individual located in a foreign country. As illustrated in the description of Carl Stoll's classic Cuckoo's Egg, the author had to go through a drawn out elaborate process in order to facilitate that individual's arrest.[51] As stated by President George Bush Jr., the treaty will help address this because it will "deny 'safe havens' to criminals, including terrorists, who can cause damage to US interests from abroad using computer systems."[52]

II) Brief introduction to fact that large number of "problem or focus areas" are not signatory countries

This study will examine if the Treaty's effectiveness may be hampered from the fact that many nations currently participating in the Treaty (signing or ratifying) are not truly the "problem countries" and cybercrime operations do not frequently originate from them. The argument is that without the nations involved where the majority of cybercrime occurs, the purpose of the Treaty is not fulfilled.[53] A way to verify or examine such a claim, is to study past well-known

---

[51] Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*.

[52] Bush, George. (2003, November 17). Letter of Transmittal. Retrieved June 30, 2004 from http://www.doj.gov/criminal/cybercrime/SenateMemo.pdf.

[53] Archik, K. (2004, July 22). *CRS Report for Congress. Cybercrime: The Council of Europe Convention.*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

instances of international cybercrime and the resulting conclusion, and to examine hypothetical situations in the current time with the Treaty factored in.

4. FOCUS: POSSIBLE EFFECTIVENESS AND IMPACT OF TREATY

A. Comparison of Non-Treaty versus Treaty Nations

A major premise of the Treaty is that by fostering international cooperation, nations can tackle the problem of the borderless nature of cybercrime by enabling pursuit beyond the borders of a single nation. However, one needs to examine which countries fall under the auspices of the Cybercrime Treaty and which do not. This should be compared against the known sources of Cybercrime to see how many nations have or have not been addressed. There are currently 18 nations that have ratified or will have the Treaty go into effect by the beginning of 2007. 17 of those nations are member nations of the Council of Europe. However an even larger 25 nations have signed but not gone on to have the Treaty go into effect (e.g. have not ratified it).[54] In addition, the Treaty also does not affect many nations outside of this Treaty.

While the United States is still the country from which the most Cybercrime attacks have originated according to the most recent Symantec Threat Report (first half of 2006), China still remains in

---

[54] Council of Europe. (2006, January 14). *Member States of the Council of Europe*. Retrieved January 14, 2007 from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

second place. In fact, China has increased in activity by 37%, which is more than double the average increase for cybercrime activity among the top nations of the world. Other nations not covered by the treaty are Canada in fourth place, Japan in eighth place, and South Korea in tenth place.[55] This makes Asia a key area for examination.

The Treaty does not include any Asian nations among its signatories, yet it accounts for 56.4% of the world's population, of which close to 400 million people utilize the Internet with a significant 245.5% growth in usage since 2000.[56] South Korea was ranked second in the second half of 2002 and fourth in the first half of 2003.[57] In 2002, Korea was considered a premier staging ground for hackers as it had a high rate of computer penetration and firmly established high-speed Internet. In fact, the Pacific Rim accounted for 91% of cyber attacks that were not traced to the U.S. at that time, with Korea accounting for 34 percent, followed by China with 29

---

[55] Symantec. *Symantec Internet Security Threat Report: Trends for January 1, 2004 – June 30, 2004*.

[56] Internet World Stats. *Internet Users and Population Statistics for Asia*. http://www.internetworldstats.com/stats3.htm. December 29, 2006.

[57] Symantec. *Symantec Internet Security Threat Report: Trends for January 1, 2004 – June 30, 2004*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

percent, 10 percent for Japan, and 7 percent for Taiwan.[58] Japan, though not present in the 2004 rankings, was ranked fourth in the last half of 2003. This perhaps should come as no surprise as Asia currently houses 25% of the world's technology suppliers, and by 2010 is forecasted to house 40% of the world's consumers of communication services.[59] Japan clearly has a more visible showing in the 2006 rankings. Despite the fact that Japan is a signatory of the Treaty, it has not gone on to ratify it as of yet. This being the case, the Treaty has no effect in Japan currently.[60]

One must also take into account that in many cases, a hacker does not necessarily live in the country of origin for an attack. It could be that the hacker is taking advantage of lax security, newer telecommunication infrastructure, or the absence of sufficient laws governing cybercrime. All these also contribute to a concern about other nations. China has the highest number of bot-infected computers worldwide, accounting for 20%.[61] Asia is also known for being a major

---

[58] Sung-jin, Y. (2002, April 26). Fwd: [ISN] Hackers Exploit Korea to Attack Global Systems." Retrieved January 14, 2007 from http://www.merit.edu/mail.archives/nanog/2002-04/msg00672.html.

[59] The Coming Asian Standards Rebellion. http://www.commsday.com.au/magazine/bandwidth/feb_mar2004/feb_mar2004_03.html. Bandwidth Magazine: May 2004.

[60] Council of Europe. (2006, January 14). *Member States of the Council of Europe*.

[61] Symantec. *Symantec Internet Security Threat Report: Trends for January 1,*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

source of spam in an age where adware, spyware, and other malicious software can easily be carried through email. According to Sophos, which tracked spam from July to September 2006, China, Japan, the Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam are all in the top 30 spam-producing countries in the world.[62] Asia is a definite consideration in its lack of participation in the Cybercrime Treaty.

In relation to the United States, there are also neighbors in the Western Hemisphere that are not a part of the Cybercrime treaty. The treaty does claim Canada, which as mentioned earlier, is ranked as a major source or cyber attacks. However, Canada has still not ratified the Treaty.[63] To the south is Mexico, and the various nations of Central America and South America. An example of the potential concerns here is the nation of Brazil. Brazil is the fifth most populous nation in the world.[64] In 2002, Brazil was considered a laboratory for Cybercrime and the world's largest exporter of it. In fact, at the time, the top ten most active hacking groups for November

---

2004 – June 30, 2004.

[62] Yeo, V. (2006, November 8). More Asian Countries Move Up Spam Ranks." ZDNet Asia. Retrieved January 14, 2007 from http://www.zdnetasia.com/news/security/0,39044215,61965497,00.htm.

[63] Council of Europe. (2006, January 14). *Member States of the Council of Europe*.

[64] Internet World Stats. *Top Ten Countries With the Highest Population*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2002 were all Brazilian.[65] In 2004, Brazil was described as the hacking capital of the world by the BBC. Statistics from security experts of other countries showed six times as many cyber attacks came out of Brazil than any other country that year. A key reason for this activity could said to be the fact that there are no serious Cybercrime laws currently in place in Brazil to properly criminalize hacking activities.[66] This situation is clearly a concern for the promotion of the Cybercrime treaty.

In Europe itself, the nation of Russia has neither signed nor ratified the Treaty. Russia however represents the largest and most populated nation in all of Europe.[67] Russia has near an estimated 24 million people with Internet access. According to the Russian Interior Ministry's Bureau for Counteracting High-Tech Crimes, Internet crime in Russia has increased to ten times as much in the past 5 years. This is partly attributed to large expansion of the Internet throughout Russia. Russian hackers have been blamed for everything from a number of computer viruses to orchestrated extortion schemes online trading protection money for averting the loss of websites.[68] It is believed

---

[65] Strahija, N. (2002, November 25). *Brazil Exports Cyber-Crime Worldwide*. Retrieved January 14, 2007 from http://www.xatrix.org/article.php?s=2291.

[66] Gibb, T. (2004, September 14). *Brazil is world 'hacking capitol*. Retrieved January 14, 2007 from http://www.ladlass.com/ice/archives/008809.html.

[67] Internet World Stats. *Top Ten Countries With the Highest Population*.

[68] Bigg, C. (2006, April 20). *Russia: Authorities Warn of Cybercrime*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

that the Russian mafia has a large hand in cybercrime within that nation. Sites are setup selling credit card numbers, Social Security numbers, PayPal and Ebay credentials, and even bank login data in large quantities. Russian language sites offer jobs for hackers to help produce malicious code. The sheer organization of the operations originating within Russia indicates a growing issue of organized cybercrime that has to be addressed within the global community.[69]

B. United States Ratification Serving as a Precedent

One possible aspect of the US ratification that needs to be examined is whether it may have an effect on the global community as a whole. Its participation can very well spur other nations into coming into accord with the Treaty. As described by one examination of international laws and relations,

…the sheer might and superpower status of the United States are such that its actions are bound to have a greater impact on the international community and on the foundations of international law. Indeed, because of the strength and dominance of the United States in almost all aspects of human endeavor, even the most insignificant

---

Epidemic. Retrieved January 21, 2007 from http://www.rferl.org/featuresarticle/2006/4/7D821779-4411-43D1-BF7B-D19743879DF6.html.

[69] Naraine, R. (2006, April 13). *Cybercrime More Widespread, Skillful, Dangerous Than Ever*. Retrieved January 14, 2007 from http://www.foxnews.com/story/0,2933,191375,00.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

changes in US foreign policy can have disproportionate and far-reaching consequences in the international community and for international law. The restraints on the United States during the Cold War period are much reduced today, and thus its influence on international relations and the international legal system is all the more obvious.[70]

However, one must also take into account the differing legal and social values that are focused upon in different nations. One major issue is that the European Union is known for much stricter privacy laws than that of the United States. It especially has a concern in dealing with the United States' Department of Homeland Security. To illustrate just how strict the EU privacy laws are, they specify that an individual must be provided with information on who is processing their data, the purpose of its processing, who has received the data, a clear means to access and correct the data, and the source of the data.[71] This difference in approach to privacy can be seen in recent occurrences.

An example of this is when the US Administration required that the EU provide access to passenger records data on Europeans flying to the U.S. These records were to contribute to an attempt to implement an

---

[70] Byers, M., Nolte, G. eds. (2003). *United States Hegemony and the Foundations of international Law*. New York: Cambridge University Press.

[71] Privacy & Data. (2006, November 7). Individual Privacy and the Law within the European Union. Retrieved January 14, 2007 from http://www.privacy-and-data.com/european-union.php.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

airline passenger profiling system known as the Computer Assisted Passenger Prescreening System (CAPPS II), which is built around a secret process of background checks and risk ratings for every person who flies. However, European privacy laws appear to be structured to disallow such disclosure and this request was denied. In December of 2003, through US negotiation, the European Commission later stated that US privacy laws were adequate. This was shortly followed however by a challenge from the European Parliament in April 2004 where it passed a resolution asking the European Court of Justice to rule on whether the agreement violates European law.[72] As it turns out, the deal between the EU and the US to transfer passenger reservation data from EU carriers to the US Department of Homeland Security was recently annulled as of September 30, 2006 by the European Court of Justice. This example clearly illustrates the difficulties of the United States in coming to terms with the stricter laws of the EU. These concerns may also play a major part in preventing the ratification of the Cybercrime Treaty by the major nations of the EU. Without the support of these signatory nations, the Treaty may lack any true force even with the involvement of the United States.[73]

---

[72] Steinhardt, B. (2004, August 13). Problem of Policy Laundering. Retrieved January 14, 2007 from http://26konferencja.giodo.gov.pl/data/resources/SteinhardtB_paper.pdf.

[73] The Policy Laundering Project. (2006, May 30). EU-US Passenger Data Transfer Deal Annulled by European Court. Retrieved January 14, 2007 from http://www.policylaundering.org/news/2006-06-12.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

C. Issues as they stand

At a glance, there are several issues that will greatly limit the effectiveness of the Cybercrime Treaty in its present state, and pose difficulty for the United States as it enters into it as a fully ratified member. The sheer numbers of non-signatory nations that are known trouble spots can create havens for hackers to operate out of to circumvent possible international cooperation fostered by this Treaty. There is also the large number of signatory nations that have not ratified the Treaty. Known reservations from many of these nations and various legal concerns may hinder some of the more developed nations of Europe from joining in ratifying the Treaty. Differing laws or in some cases the absence of laws dealing with Cybercrime in many nations also create difficulty to properly prosecute Cybercrime. The last section of this study will broach the inherent problems of a "borderless Internet" and whether all these issues may possible render such a Treaty ineffective in its operation.

5. ILLUSTRATIVE SCENARIOS

A. Past Example of How the Treaty Would Not Have Affected

A past scenario to illustrate where the Treaty would not have had an effect, is the ILOVEYOU virus that caused an estimated 10 billion dollars in damage when it was released in 2000. The Philippines is neither a signatory country, nor did it have laws established at the time to deal with such an issue of cybercrime. However, this widespread virus affected the United States and other signatory countries of the Cybercrime Treaty. The author of the virus, Onel de Guzman, was from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the Philippines and there was little that the United States was able to do once they tracked him. Despite the fact that anti-cybercrime laws were enacted by the Philippines after the fact, it could not be applied to de Guzman's case.[74] Other countries that are known for their high level of technology and telecommunications (e.g. South Korea) are hotbeds of hacker activity, and are currently not included in the Treaty. The Treaty is meant to allow for pursuit and extradition of cyber-criminals from wherever they may hide. Unfortunately, there are still many "safe havens" from which criminals can commit offenses that would not fall under the auspices of even a fully ratified Treaty.

Another example that is more recent is a Denial of Service attack within England that could not be prosecuted due to lack of specification within the law. A London teen caused a Denial of Service by sending 5 million emails. The Computer Misuse Act passed in 1990 for the UK does not criminalize this type of behavior. The Act targets three types of offenses, which are unauthorized access to computer material, unauthorized modification of such material; and unauthorized access with intent to commit or facilitate commission of further offences. It was argued that though email being received does access and modify data stored in the computer's random access memory. However, email was argued to be an authorized access. Since this was not a distributed denial of service attack (in which case it could be argued other computers were illegally accessed), the Act did not hold

---

[74] Kelsey, D. (2000, June 30). *"Love Bug" Suspect Charged in Philippines*. Retrieved June 25, 2004 from http://www.computeruser.com/news/00/06/30/news4.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the teenager liable.[75] It is issues such as this that show the tricky nature of establishing Cybercrime laws. Though this situation was internal in nature, it could still apply in any situation where an attack was launched from another nation using a bombardment of emails, especially if that nation also did not have much Cybercrime law support.

B. Hypothetical Example of Circumvention

To properly illustrate how the United States could be attacked by cybercrime activity without any benefit from the Cybercrime Treaty, one could imagine various scenarios. For the purpose of this study, one hypothetical example will be presented. A terrorist (or a simple enterprising businessman with hacking ability) decides to set up activity in Indonesia. While a hacker could operate anywhere and go through another nation, the operative in this case sets up shop here to improve physical security and reduces the odds of being easily removed (or located). According to a report released by the Office of the Coordinator for Counterterrorism, Indonesia remains "difficult to control" by its government, "surveillance is partial at best, and traditional smuggling and piracy groups provide an effective cover for

[75] Out-Law News. (2005, March 11). Denial of Service prosecution fails. Retrieved January 14, 2007 from http://www.out-law.com/page-6298.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

terrorist activities in the area."[76] He decides to exploit a computer in Taiwan to base his attacks. Taiwan has experienced a large explosion of technological growth with a 60% internet penetration of the population. However it is known to be one of the top 10 countries to have its computers become zombie-infected per capita.[77] The hacker could set up a command and control server from here. Instead of taking advantage of Taiwan's bot-infected network however, the hacker would target Mainland China. China is known to be the number one country as far as number of bot-infected networks (within the first half of 2006) and next to the United States, leads as having the most cyber-attacks originating from it.[78] There is also the chance that a bot network is already in place, and the attacker could take advantage of that to implement his attack.

In introducing this layer of nations between the target and the hacker, the hacker would not only be taking advantage of existing bot-infrastructure in place, but also a historic animosity between Taiwan and China. Taiwan has pushed for equal recognition and status as mainland China, whereas China has in the past considered Taiwan as a

---

[76] U.S. Department of State. (2006, April 28). Country Reports on Terrorism. Retrieved January 14, 2007 from http://www.state.gov/s/ct/rls/crt/2005/64333.htm.

[77] Morel, B. (2006, May 15). A Methodology for Measuring the Capability to Counter Cybersecurity-Related Offenses. (Carnegie Mellon University).

[78] Symantec. *Symantec Internet Security Threat Report: Trends for January 1, 2004 – June 30, 2004*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

rebellious province. This animosity has led to various cyber attacks on both sides, including a hacker war between the two going as far back as 1999 in which both had groups of hackers penetrating and defacing or damaging websites belonging to the opposing group.[79] The level of cooperation needed between these nations in tracing an attack and ascertaining the details could greatly hinder US investigative powers.

This scenario then has the added fact that the target is not the United States directly, but the nation of India. In 2005 alone, financial services made up 39 percent outsourced companies in the nation India. TowerGroup reports that the top 15 global financial institutions will increase IT spending on vendor-direct offshore outsourcing by 34 percent annually, to $3.89 billion in 2008.[80] Furthermore, 82% of US companies ranked India as their number one choice for software outsourcing.[81]

However some security testers feel India still has weak security despite a drive to increase security. Security testing of India high

---

[79] Laris, M. (1999, September 13). Hackers Are Front-Line Troops in This China-Taiwan Conflict." Retrieved January 14, 2007 from http://seclists.org/isn/1999/Sep/0012.html.

[80] Krebsbach, K. (2007). Inside the Outsourcing World of India. Retrieved January 14, 2007 from http://www.banktechnews.com/article.html?id=20070102SM9O2E2D.

[81] Global Solutions. (n.d.) Why Outsource to India? Retrieved January 14, 2007 from http://www.globalsolutionindia.com/outsourceindia.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

tech firms has revealed weak security.[82] Over 4, 000 Indian websites were hacked as recently as November 2006. Half of which were .com sites.[83] In a study, only "thirty-five percent of India-based respondents reported they used secure remote access (vs. the rest of the world at 56 percent and the U.S. at 62 percent). Only half of organizations in India employ the basics such as user passwords (vs. the rest of the world at 73 percent and the U.S. at 78 percent), and 50 percent admit more than half their users are not in compliance with their information security policies."[84]

Given the number of companies that outsource to India, and the possible tentative nature of security in India, this could directly impact US businesses. A denial of service could be a crippling blow to financial organizations in the United States, given that transactions and financial deals are done electronically every minute in the United

---

[82] Kirby, C. (2004, March 28). *Hacking danger for outsourced records hard to gauge*. Retrieved January 14, 2007 from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/03/28/MNG573MCQG25.DTL.

[83] Chatterjee, M. B. (2006, December 25). *4,000 Indian websites hacked: MHA*. Retrieved January 14, 2007 from http://economictimes.indiatimes.com/4000_Indian_websites_hacked_MHA/articleshow/916304.cms.

[84] Price Waterhouse Coopers. (n.d.) *New Survey Shows Physical and Information Security Convergence is Increasing; India Lags But is Closing Gaps in Security*. Retrieved January 14, 2007 from http://www.pwc.com/extweb/ncpressrelease.nsf/docid/ACE3B75B1B91492E852571EA0050DE76.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

States. If the hacker specifically targets US financial interests outsourced to India, the denial of service could result in tremendous financial loss. While it would be very difficult to estimate the amount of money lost from a denial of service attack, one need to simply consider how much money is traded or exchanged in a period of time. A large company can deal in millions of dollars a day, making even a single day of downtime costly. One Fortune 500 company even calculated it lost around $10 million dollars to the Melissa virus.[85] One can see how this scenario could cost the United States a great deal of money, yet none of the many countries involved in this scenario are at all covered by the Cybercrime Treaty.

C. Past Example Where International Cooperation Succeeded

The concepts addressed in the Cybercrime Treaty are not original. In fact, the first court-ordered real-time monitoring of an unknown subject in order to catch a cyber criminal was initiated over a decade ago in 1995. In July of 1995, there were intrusions reported by several states and Mexico that seemed to be originating from Harvard University. By August, the intrusions had escalated to an intrusion into a government network operated by the U.S. Naval Command, Control and Ocean Surveillance Center (NCCOSC). The hacker was attempting to capture user id's and passwords via a sniffer program. Working in cooperation with the network manager of Harvard Arts and Sciences

---

[85] Power, R. (n.d.)The Financial Costs of Computer Crime. Retrieved January 14, 2007 from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/cost.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Computer services, the Naval Criminal Investigative Service managed to trace the hacker and his online identity to Argentina. Using unique names utilized by the hacker and other key words, a profile was created which resulted in the obtaining of a wire-tap order. Argentine authorities carried out the arrest of Julio Cesar Ardita and seized his computer.

As one can see, the concepts presented by the Cybercrime Treaty are within established precedent and current law. The Ardita case also helps illustrate the importance of the Cybercrime Treaty as the Ardita case was greatly impeded due to the lack of any international agreements that dealt with extradition for cyber crimes at that time.[86] Article 19 of the Treaty also lays out that stringent conditions and safeguards are needed for real-time interception of data due to the fact that it is a "very intrusive measure on private life," and refers to other Articles and sections, which also provide for safeguards.[87] The Cybercrime Treaty will use existing law enforcement methods but remove longstanding procedural obstacles. Though Argentina is not currently a signatory nation, it helps illustrate what can be achieved through cooperation, and supports the concept of facilitated international assistance, especially when law enforcement agencies from

---

[86] Counter Intelligence Awareness Guide. (n.d.) *Hacking U.S. Government Computers from Overseas*. Retrieved January 14, 2007 from http://www.ntc.doe.gov/cita/CI_Awareness_Guide/Spystory/Hacking.htm#1.

[87] Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

each nation can deal directly with each other.

6. CONCLUSION

The Council of Europe Convention on Cybercrime Treaty is not a panacea to cure the world of cybercrime with its simple existence. Most of the major nations of Europe, which comprise the majority of Treaty signatories, have not ratified it, reflecting strong concerns on privacy, human rights, and other reservations possibly giving pause to many nations in fully ratifying this treaty. Several nations long thought to be "havens" for hacker-activity are not even a part of the Treaty. A strong possibility exists that cybercrime could still be conducted around the laws in place if the nations were all to ratify it, as there truly is a borderless nature to the Internet.

However, it can also be seen from examining the past and present, that often cybercrime is not prevented due to a lack of properly structured laws in place until after the fact. The world as a whole has been of a more reactive nature instead of a proactive one. Laws are made in many countries after an act of cybercrime is committed because it could not be prosecuted. While the argument can be made that the Cybercrime Treaty will not manage to achieve its goals by itself, it still represents a very progressive approach to Cybercrime. Universalizing laws so that nations anticipate crimes ahead of time instead of correcting them after the fact is an important stride in handling Cybercrime. Opening channels of communication and removing much of the bureaucratic red tape that hinders investigations would greatly enhance global incident handling.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Whether or not the Cybercrime Treaty will be able to achieve all it sets out too, a world-wide approach to incident-handling and Cybercrime is vital if the growing threat of global cybercrime is to be met. It is hard to determine whether amendments to the Treaty in response to the demands of citizens or changes to various governments' approach to cybercrime itself will enable the Treaty to succeed. The Cybercrime Treaty could also be expanded to include other nations or set the groundwork for an even more encompassing international treaty. If the Cybercrime Treaty turns out to be incapable of accomplishing its goal on its own, the Cybercrime Treaty can still be seen as the first true step toward a universal approach to dealing with cybercrime and an attempt to truly foster cooperation among nations.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

7. REFERENCES

The American Civil Liberties Union. (n.d.) *8 Reasons for US to Reject the International Cyber Crime Treaty*. Retrieved January 21, 2007 from http://www.totse.com/en/law/justice_for_all/165280.html.

Archik, K. (2004, July 22). *CRS Report for Congress. Cybercrime: The Council of Europe Convention*. Retrieved January 21, 2007 from http://fpc.state.gov/documents/organization/36076.pdf.

BBC News. (2000, December 18). *Cybercrime Treaty Condemned*. Retrieved January 21 from, 2007 from http://news.bbc.co.uk/1/hi/sci/tech/1072580.stm.

Bigg, C. (2006, April 20). *Russia: Authorities Warn of Cybercrime Epidemic*. Retrieved January 21, 2007 from http://www.rferl.org/featuresarticle/2006/4/7D821779-4411-43D1-BF7B-D19743879DF6.html.

Bush, George. (2003, November 17). *Letter of Transmittal*. Retrieved June 30, 2004 from http://www.doj.gov/criminal/cybercrime/SenateMemo.pdf.

Business Software Alliance. *BSA Comments on Convention*. (2000, September 8). Retrieved June 25, 2004 from http://global.bsa.org/security/resources/2000-09-08/06.doc.

Byers, M., Nolte, G. eds. (2003). *United States Hegemony and the Foundations of international Law*. New York: Cambridge University Press.

Cert Coordination Center. (2004). *2004 eCrimeWatch Survey Summary of Findings*. Retrieved January 21, 2007 from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf.

Chatterjee, M. B. (2006, December 25). *4,000 Indian websites hacked: MHA*. Retrieved January 14, 2007 from http://economictimes.indiatimes.com/4000_Indian_websites_hacked_MHA/articleshow/916304.cms.

Council of Europe. (2006, January 14). *Member States of the Council of Europe*. Retrieved January 14, 2007 from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

Counter Intelligence Awareness Guide. (n.d.) *Hacking U.S. Government Computers from Overseas*. Retrieved January 14, 2007 from http://www.ntc.doe.gov/cita/CI_Awareness_Guide/Spystory/Hacking.htm#1.

The Department of Justice. (2003, November 10). *Frequently Asked Questions and Answers: Council of Europe Convention on Cybercrime*. Retrieved January 14, 2007 from http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA11.

Dick Kelsey. (2000, June 30). *'Love Bug' Suspect Charged In Philippines*. Retrieved January 14, 2007 from http://www.computeruser.com/news/00/06/30/news4.html.

Electronic Privacy Information Center. (2004, June 17). *Letter to Richard G. Lugar and Joseph R. Biden, Jr.* Retrieved January 14, 2007 from http://www.epic.org/privacy/intl/senateletter-061704.pdf.

Gibb, T. (2004, September 14). *Brazil is world 'hacking capitol*. Retrieved January 14, 2007 from http://www.ladlass.com/ice/archives/008809.html.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Global Internet Liberty Campaign. (2000, October 18). *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*. Retrieved January 14, 2007 from http://www.gilc.org/privacy/coe-letter-1000.html.

Global Lawful Interception Forum. (n.d.) *Eight Reasons the US Should Ratify the Cybercrime Treaty*. Retrieved January 14, 2007 from http://www.gliif.org/RafityNow/reasons.htm.

Global Solutions. (n.d.) *Why Outsource to India?* Retrieved January 14, 2007 from http://www.globalsolutionindia.com/outsourceindia.html

Golubev, V. (2004, June 16). *International Cooperation in Fighting Transnational Computer Crime.* Retrieved January 14, 2007 from http://www.crime_research.org/articles/431/.

Internet World Stats. (2006, December 29). *Internet Users and Population Statistics For Asia*. Retrieved January 14, 2007 from http://www.internetworldstats.com/stats3.htm.

Internet World Stats. (2005, December 31). *Top Ten Countries With the Highest Population*. http://www.internetworldstats.com/stats8.htm.

Kelsey, D. (2000, June 30). "Love Bug" Suspect Charged in Philippines. Retrieved June 25, 2004 from http://www.computeruser.com/news/00/06/30/news4.html.

Kirby, C. (2004, March 28). *Hacking danger for outsourced records hard to gauge*. Retrieved January 14, 2007 from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/03/28/MNG573MCQG25.DTL.

Krebsbach, K. (2007). *Inside the Outsourcing World of India*.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Retrieved January 14, 2007 from http://www.banktechnews.com/article.html?id=20070102SM9O2E2D.

Laris, M. (1999, September 13). *Hackers Are Front-Line Troops in This China-Taiwan Conflict*." Retrieved January 14, 2007 from http://seclists.org/isn/1999/Sep/0012.html.

Legal Affairs Treaty Office. (2001, November 23). *Council of Europe Convention on Cybercrime*. Retrieved September 1, 2007 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Leydon, J. (2005, November 29). *Cybercrime 'more lucrative' than drugs*. Retrieved January 14, 2007 from http://www.channelregister.co.uk/2005/11/29/cybercrime/.

Lugar, R. (2004, June 17). *Committee on Foreign Relations United States Senate Hearing*. Retrieved January 14, 2007 from http://www.senate.gov/~foreign/hearings/2004/hrg040617a.html.

The Maudit Group. (n.d.). *Glossary and Acronyms - International Business - Con to D*. Retrieved January 14, 2007 from http://www.rmauduit.com/glossary-con.html.

McConnell International. (2000).*Cyber Crime … and Punishment? Archaic Laws Threaten Global Information*." Retrieved January 14, 2007 from http://www.library.cornell.edu/colldev/mideast/cycrime.pdf.

McCullagh, D. (2003, November 18). *President Bush has asked the US Senate to ratify the first international cybercrime treaty*. Retrieved January 14, 2007 from http://news.zdnet.com/2100-1009_22-5108854.html.

McCullagh, D & Broache, A. (2006, August 4). *Senate Ratifies*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Controversial Cybecrime Treaty. Retrieved January 14, 2007 from http://news.com.com/Senate+ratifies+controversial+cybercrime+treaty/2100-7348_3-6102354.html. CNET.

Meinel, C. (2004). International Convention on Cybercrime Could Chill Computer Security Research. *Security & Privacy*, Vol. 2 (No. 4), 28-32.

Morel, B. (2006, May 15). *A Methodology for Measuring the Capability to Counter Cybersecurity-Related Offenses*. (Carnegie Mellon University).

Naraine, R. (2006, April 13). *Cybercrime More Widespread, Skillful, Dangerous Than Ever*. Retrieved January 14, 2007 from http://www.foxnews.com/story/0,2933,191375,00.html. A

Out-Law News. (2005, March 11). *Denial of Service prosecution fails*. Retrieved January 14, 2007 from http://www.out-law.com/page-6298.

The Policy Laundering Project. (2006, May 30). *EU-US Passenger Data Transfer Deal Annulled by European Court*. Retrieved January 14, 2007 from http://www.policylaundering.org/news/2006-06-12.html.

Powell, C. (2003, September 11). *Letter of Submittal*. Retrieved June 30, 2004 from http://www.usdoj.gov/criminal/cybercrime/senateMemo.pdf.

Power, R. (n.d.)*The Financial Costs of Computer Crime*. Retrieved January 14, 2007 from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/cost.html.

Price Waterhouse Coppers. (n.d.) *New Survey Shows Physical and Information Security Convergence is Increasing; India Lags But is Closing Gaps in*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Security. Retrieved January 14, 2007 from http://www.pwc.com/extweb/ncpressrelease.nsf/docid/ACE3B75B1B91492E852571EA0050DE76.

Privacy & Data. (2006, November 7). *Individual Privacy and the Law within the European Union*. Retrieved January 14, 2007 from http://www.privacy-and-data.com/european-union.php.

Rizvi, H. (2004, January 21). *Bush's Plan to Increase Internet Surveillance*. Retrieved June 30, 2004 from http://www.alternet.org/rights/17633.

Roger, W. (2001, June 26). *Cybercrime treaty raises privacy and commerce questions*. Retrieved January 14, 2007 from http://techrepublic.com.com/5100-6298_11-1040577.html.

SANS. *Incident Handling Step-by-Step and Computer Crime Investigation*. (The Sans Institute, 2006), 6-7.

Sarkar, A. (2004, August 24). *The Cuckoo's Egg by Clifford Stoll*. Retrieved January 14, 2007 from http://www.cs.sfu.ca/~anoop/weblog/archives/000052.html.

Senate Foreign Relations Committee. (2004, June 17). *Statement of Bruce Swartz; Deputy Assistant Attorney General; Criminal Division; Multilateral Law Enforcement Treaties*. Retrieved January 14, 2007 from http://foreign.senate.gov/testimony/2004/SwartzTestimony040617.pdf.

Steinhardt, B. (2004, August 13). *Problem of Policy Laundering*. Retrieved January 14, 2007 from http://26konferencja.giodo.gov.pl/data/resources/SteinhardtB_paper.pdf.

Stoll, C. *The Cuckoo's Egg: Tracking a Spy Through the Maze of*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Computer Espionage. New York: Pocket Books, 1990.

Strahija, N. (2002, November 25). *Brazil Exports Cyber-Crime Worldwide*. Retrieved January 14, 2007 from http://www.xatrix.org/article.php?s=2291.

Sung-jin, Y. (2002, April 26). *Fwd: [ISN] Hackers Exploit Korea to Attack Global Systems*." Retrieved January 14, 2007 from http://www.merit.edu/mail.archives/nanog/2002-04/msg00672.html.

Symantec. *Symantec Internet Security Threat Report: Trends for January 1, 2004 – June 30, 2004*. Volume IV, September 2004.U.S. Department of State. (2006, April 28). *Country Reports on Terrorism*. Retrieved January 14, 2007 from http://www.state.gov/s/ct/rls/crt/2005/64333.htm.

Watson, D. (2006, June 7). *IPR Issues and Dangers of Counterfeited Goods Imported into the U.S*. Retrieved January 14, 2007 from http://www.uscc.gov/hearings/2006hearings/written_testimonies/06_06_07wrts/06_06_7_8_watson_diane.php.

Yeo, V. (2006, November 8). *More Asian Countries Move Up Spam Ranks*." ZDNet Asia. Retrieved January 14, 2007 from http://www.zdnetasia.com/news/security/0,39044215,61965497,00.htm.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced