

**Background Guide Topic Three:**  
**Prevention and protection against cybercrime**

*Introduction*

The war on cybercrime is different and less successful than other efforts to eliminate crime because the criminals are essentially unknown actors. Where most criminals will leave a trace of themselves at the scene of a crime, the internet offers cybercriminals the option to remain completely anonymous.<sup>1</sup> Additionally, cybercriminals are able to network easily with like-minded individuals around the globe through the World Wide Web.<sup>2</sup> As to the question of the primary prevention and prosecution actors, each state may have its own, but currently no international organ exists to primarily fight cybercrime.

The realm of cybercrime is broad and not easily defined. The World English Dictionary defines cybercrime as “the illegal use of computers and the internet” or “crime committed by means of computers or the internet.”<sup>3</sup> The United Nations Office on Drugs and Crime (UNODC) identifies the following as types of cybercrime: hacking (“offences against computer data and systems”), phishing (“computer- related forgery and fraud”), child pornography and other content offenses, and copyright offenses such as illicit downloads and uploads.<sup>4</sup> Other offenses fall under the title of cyberterrorism. These offenses threaten the security of states through the remote penetrations of power grids, air trafficking installations, and nuclear installations.<sup>5</sup> Cyberattacks have even been conducted on government systems – such as those in the United States and in the Republic of Korea.<sup>6</sup>

The issue of cybercrime and cybersecurity becomes even more conflicting when one state launches a cyberattack upon another: a phenomenon often identified as cyberwar. The legality of cyberwar is questionable, as most UN Member States signed a treaty amendment in the 1990s stating that states are not to cause “technical harm ... to the operation of ... telecommunication services of other ... States”

---

<sup>1</sup> “Cybercrime.” *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. New York: United Nations Publications, 2010. 201-218. Print. <<http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>>.

<sup>2</sup> Idem.

<sup>3</sup> “Cybercrime.” *Collins English Dictionary - Complete & Unabridged 10th Edition*. HarperCollins Publishers. Web. 7 September 2010. Dictionary.com <<http://dictionary.reference.com/browse/cybercrime>>.

<sup>4</sup> “Cybercrime.” *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. New York: United Nations Publications, 2010. 201-218. Print. <<http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>>.

<sup>5</sup> “Organized Crime Has Globalized and Turned into a Security Threat.” *UNODC*. United Nations Office on Drugs and Crime. 17 June 2010. Web. 5 September 2010. <<http://www.unodc.org/unodc/en/press/releases/June/organized-crime-has-globalized-and-turned-into-a-security-threat.html>>.

<sup>6</sup> “New cyberattacks in SKorea; sites suffer no damage.” *KSTP TV*. Associated Press, 13 June 2010. Web. 15 June 2010. <<http://kstp.com/news/stories/S1023779.shtml?cat=159>>.

and should “recognize the necessity of taking practical measures to prevent ... disrupting the operation of telecommunication installations within the jurisdiction of other Member States.”<sup>7</sup> Israel, however, announced that cyberwar may be necessary to deter aggressive nations.<sup>8</sup> Israel suggested the Middle Eastern state could implement this policy against the Islamic Republic of Iran.<sup>9</sup>

Cybercrime is a growing phenomenon that must be halted. The number of cyberattacks – both on individuals and on regimes – grows exponentially for each new cybercriminal.<sup>10</sup> Currently no international treaty or regime expressly addresses the growing dangers of cybercrime, nor do most developing and transitional states have the means to defend against cybercrimes.<sup>11</sup> If the threat is not addressed quickly, cybercrime could easily destroy the lives of millions – if not billions – of innocent individuals.

### *History*

The late 1970s saw the development of a computing program intended to identify underused processors.<sup>12</sup> This benign program was the ancestor of the modern malicious computer worm.<sup>13</sup> This was the first instance of computer program that could be used to infiltrate and harm multiple computers connected on a network. The 1980s introduced a wave of threats to the developing computer world: a group of young American hackers attempted to break into secure computer systems – including at least one government system –, the first PC computer virus – known as “The Brain” – was developed by two brothers in Pakistan, and an American graduate student released a computer virus on one of the internet’s precursors disabling thousands of computers and systems.<sup>14</sup> After the World Wide Web gave the public access to the Internet in 1990, cyberattacks skyrocketed. Russian Vladimir Levin stole several million dollars from Citibank online, Kevin Mitnick stole top secret files from Motorola and

---

<sup>7</sup> Rutowski, A.M. “Is cyberwar lawful?” *Computerworld*. Computerworld, Inc., 9 August 2010. Web. 10 August 2010. <[http://www.computerworld.com/s/article/9180469/Is\\_cyberwar\\_lawful\\_](http://www.computerworld.com/s/article/9180469/Is_cyberwar_lawful_)>.

<sup>8</sup> Greene, Tim. “Quiz: Separate cyber security fact from fiction.” *Network World*. Network World Inc., 15 October 2009. Web. 7 September 2010. <<http://www.networkworld.com/slideshows/2009/101609-cybersecurity-quiz.html#>>.

<sup>9</sup> Idem.

<sup>10</sup> “Cybercrime.” *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. New York: United Nations Publications, 2010. 201-218. Print. <<http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>>.

<sup>11</sup> Idem.

<sup>12</sup> Keefe, Mari. “A short history of hacks, worms and cyberterror.” *Computerworld*. Computerworld Inc., 27 April 2009. Web. 10 September 2010.

<[http://www.computerworld.com/s/article/9131924/A\\_short\\_history\\_of\\_hacks\\_worms\\_and\\_cyberterror?taxonomyId=13&pageNumber=1&taxonomyName=Government](http://www.computerworld.com/s/article/9131924/A_short_history_of_hacks_worms_and_cyberterror?taxonomyId=13&pageNumber=1&taxonomyName=Government)>.

<sup>13</sup> Idem.

<sup>14</sup> Idem.

Sun Microsystems, a group of hackers spent a period of five months breaking into secure American government websites and altering information, the Solar Sunrise attacks led investigators to believe a series of cyberattacks originated in Iraq, and the “Melissa” worm causes \$1.5 billion of damages on thousands of computers.<sup>15</sup> The twenty-first century has seen an influx of computer worms and a growing number of hackers around the world: Microsoft Corporation was infiltrated by Russian hackers; Amazon, Yahoo!, and eBay were knocked offline for several hours due to cyberattacks; the ILOVEYOU worm, Anna Kournikova virus, Klez worm, Slammer worm, and My Doom worm each infected millions of computers with malicious viruses and dangerous pictures of Russian tennis players; a Russian hacker group – the Hang-Up Team – published tools for hacking the websites of financial institutions online; the Democratic People’s Republic of Korea (DPRK) claimed to have trained several hundred hackers to infiltrate the Japanese and Republic of Korea (ROK) government systems; the Shadowcrew Web team operated a whistle-blowing website from six different countries; and a Turkish hacker broke into the United Nations website.<sup>16</sup>

Two of the most famous cyberattacks in the last two decades occurred in the former Soviet republics of Estonia and Georgia. In early 2007, the Estonian government decided to relocate a Soviet war monument sparking outrage from the Russian nationals living within Estonia.<sup>17</sup> The attack, which began in late April, consisted of two types of cyberattacks: botnets<sup>18</sup> and distributed denial of service (DDoS) onslaught.<sup>19</sup> Botnets are groups of computers that have been affected by malicious computing software.<sup>20</sup> Cybercriminals can remotely access botnets and often use the affected computers to perform various crimes and actions, including DDoS attacks.<sup>21</sup> DDoS attacks occur when botnets are programmed to constantly attempt to request certain websites for information, overloading the websites

---

<sup>15</sup> Idem.

<sup>16</sup> Idem.

<sup>17</sup> Anderson, Nate. “Massive DDoS attacks target Estonia; Russia accused.” *Security. Ars Technica*, 14 May 2007. Web. 8 September 2010. <<http://arstechnica.com/security/news/2007/05/massive-ddos-attacks-target-estonia-russia-accused.ars>>.

<sup>18</sup> Kirk, Jeremy. “Estonia recovers from massive DDoS attack.” *Computerworld*. Computerworld Inc., 17 May 2007. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9019725/Estonia\\_recovers\\_from\\_massive\\_DDoS\\_attack](http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack)>.

<sup>19</sup> Anderson, Nate. “Massive DDoS attacks target Estonia; Russia accused.” *Security. Ars Technica*, 14 May 2007. Web. 8 September 2010. <<http://arstechnica.com/security/news/2007/05/massive-ddos-attacks-target-estonia-russia-accused.ars>>.

<sup>20</sup> Kirk, Jeremy. “Estonia recovers from massive DDoS attack.” *Computerworld*. Computerworld Inc., 17 May 2007. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9019725/Estonia\\_recovers\\_from\\_massive\\_DDoS\\_attack](http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack)>.

<sup>21</sup> Idem.

and shutting them down.<sup>22</sup> The origins of DDoS attacks are difficult to ascertain because of the use of botnets that include computers from dozens of countries. The botnet used in the Estonia attack consisted of computers in Canada, Brazil, the United States, and Vietnam amongst other countries.<sup>23</sup> Many claim that the cyberattack which shut down numerous Estonian government websites for several days originated in Russia, and possibly with the Russian government.<sup>24</sup> The North Atlantic Treaty Organization (NATO) sent several observers to monitor the crisis in Estonia who were not able to conclusively determine the origins of the attack.<sup>25</sup>

During the 2008 crisis in Georgia regarding the South Ossetia and Abkhazia secessions, the former Soviet republic faced a cyberattack with the message “win+love+in+Russia.”<sup>26</sup> The DDoS attack on Georgia began in late July before the Russian troops entered Georgia.<sup>27</sup> Government sites, such as that of President Mikheil Saakashvili, crashed for at least twenty four hours due to the onslaught of activity.<sup>28</sup> Other targets included communications, media, and transportation companies’ websites.<sup>29</sup> While the command server was believed to be within the United States, many Georgian officials claimed the attack originated from Russian nationals and possibly the Russian government.<sup>30</sup> If the government of the Russian Federation has indeed ordered the cyberattack, this event could be considered the first act of cyberwar as it would be the first cyberattack to coincide with a militarized conflict.<sup>31</sup> Even after the end of the attack, a Russian-language website – stopgeorgia.ru – posted downloadable instructions and software for DDoS attacks.<sup>32</sup>

International cyberattacks haven’t only attempted to hinder governments, but infiltrate secure government systems and either steal state secrets or perform acts of sabotage. From about 2004 until

---

<sup>22</sup> Idem.

<sup>23</sup> Idem.

<sup>24</sup> Anderson, Nate. “Massive DDoS attacks target Estonia; Russia accused.” *Security. Ars Technica*, 14 May 2007. Web. 8 September 2010. <<http://arstechnica.com/security/news/2007/05/massive-ddos-attacks-target-estonia-russia-accused.ars>>.

<sup>25</sup> Idem.

<sup>26</sup> Markoff, John. “Global Monitor - Cyber attacks on Georgia signal a new kind of warfare.” *Scotland on Sunday*. Johnston Press Digital Publishing, 17 August 2008. Web. 10 September 2010. <<http://scotlandonsunday.scotsman.com/business/Global-Monitor---Cyber.4398541.jp>>.

<sup>27</sup> Idem.

<sup>28</sup> Idem.

<sup>29</sup> Idem.

<sup>30</sup> Idem.

<sup>31</sup> Idem.

<sup>32</sup> Idem.

about 2008, an espionage ring known as GhostNet spied on over 1200 computers in 103 countries.<sup>33</sup> A ten-month cyberespionage investigation discovered evidence that numerous embassies, government officials, and non-governmental groups were affected by the spyware.<sup>34</sup> The foreign ministries of Bangladesh, Barbados, Bhutan, Brunei, Indonesia, Iran, Latvia, and the Philippines were considered “high-risk” infiltrations in the investigation report with embassies of Cyprus, Germany, India, Indonesia, Malta, Pakistan, Portugal, Romania, the ROK, Taiwan, and Thailand also affected.<sup>35</sup> Computer systems for the secretariat of the Association of Southeast Asian Nations (ASEAN), the South Asian Association for Regional Cooperation (SAARC), the Asian Development Bank, and NATO all exhibited signs of infiltration by GhostNet.<sup>36</sup> Private businesses, especially media organs such as the Associated Press, were also targeted by the espionage ring.<sup>37</sup> Tibet experienced the highest number of infected computers: the group targeted the Tibetan government in exile, several Tibetan nongovernmental organizations, and the office of the Dalai Lama.<sup>38</sup> The hackers with GhostNet used the forced access to view confidential documents and to control computer microphones and webcams to observe the areas around the infected computers.<sup>39</sup> Reports and rumors began circulating, after the completion of the investigation, claiming the Chinese government was responsible for the actions of the cyberespionage ring. States are often considered the actors most likely to use cyberterrorist attacks, such as cyberespionage, because they have the necessary access to resources and trained professionals and have the necessary commitment and will.<sup>40</sup> China, however, vehemently denied the claims, arguing that China is opposed to hacking and other cyberattacks.<sup>41</sup> Supporting his government, a Chinese businessman claimed that the software used by GhostNet was unsophisticated and a Chinese hacker would use more sophisticated, previously unseen software.<sup>42</sup>

Chinese nationals, and possibly the Chinese government, were also implicated as the origins of a

---

<sup>33</sup> Kirk, Jeremy. “Deep computer-spying network touched 103 countries.” *Computerworld*. Computerworld Inc., 29 March 2009. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9130704/Deep\\_computer\\_spying\\_network\\_touched\\_103\\_countries](http://www.computerworld.com/s/article/9130704/Deep_computer_spying_network_touched_103_countries)>.

<sup>34</sup> Idem.

<sup>35</sup> Idem.

<sup>36</sup> Idem.

<sup>37</sup> Idem.

<sup>38</sup> Idem.

<sup>39</sup> Fletcher, Owen. “China denies cyberspy network charges.” *Computerworld*. Computerworld Inc., 31 March 2009. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9130804/China\\_denies\\_cyberspy\\_network\\_charges](http://www.computerworld.com/s/article/9130804/China_denies_cyberspy_network_charges)>.

<sup>40</sup> Greene, Tim. “Quiz: Separate cyber security fact from fiction.” *Network World*. Network World Inc., 15 October 2009. Web. 7 September 2010. <<http://www.networkworld.com/slideshows/2009/101609-cybersecurity-quiz.html#>>.

<sup>41</sup> Fletcher, Owen. “China denies cyberspy network charges.” *Computerworld*. Computerworld Inc., 31 March 2009. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9130804/China\\_denies\\_cyberspy\\_network\\_charges](http://www.computerworld.com/s/article/9130804/China_denies_cyberspy_network_charges)>.

<sup>42</sup> Idem.

cyberespionage scheme in 2003 and 2004 known as Titan Rain.<sup>43</sup> The objective of Titan Rain was the theft of sensitive documents from the government of the United States, especially classified military documents.<sup>44</sup> Cyberspies used a program to scan the computers on a network and identify those computers with weaknesses for future exploitation.<sup>45</sup> One means the hackers used to access the secure networks was the use of thumb drives. These could be dropped in a parking lot or a restroom and anyone finding the thumb drive would presumably insert the device into their own computer in an attempt to identify the owner. However, as soon as the thumb drive is inserted, the spyware downloads itself onto the computer giving the hackers access to the system. This method, in addition to others, was used to access the United States Department of Defense, Department of Justice, Army Systems Engineering Command, Naval Ocean Systems Center, Army Space and Strategic Defense installation, and Pentagon.<sup>46</sup> Similar attacks, also allegedly originating in China, have been reported by German Chancellor Angela Merkel and by the government of the United Kingdom – specifically: Whitehall, the House of Commons, MI5, and the Centre for the Protection of the National Infrastructure in the Cabinet Office.<sup>47</sup> The United Kingdom believes the cyberattacks on its government networks were performed in conjunction with the People’s Liberation Army (PLA).<sup>48</sup>

### *Current Situation*

In 2004, 23 year old Albert Gonzalez provided the United States government with details necessary to collapse the Shadowcrew Web group.<sup>49</sup> Shadowcrew had stolen 1.5 million credit card and ATM numbers online and Gonzalez’s information resulted in twenty eight arrests.<sup>50</sup> At the time, Gonzalez was considered one of the leaders of the Shadowcrew ring, but received government immunity for acting as an informant.<sup>51</sup> Five years later in 2009, Gonzalez was indicted by a federal grand jury for a

---

<sup>43</sup> Thornburgh, Nathan. “Titan Rain: Chinese Cyberespionage?.” *Time*. Time Inc., 25 August 2005. Web. <<http://www.time.com/time/nation/article/0,8599,1098371,00.html>>.

<sup>44</sup> *Idem*.

<sup>45</sup> *Idem*.

<sup>46</sup> *Idem*.

<sup>47</sup> Norton-Taylor, Richard. “Titan Rain – how Chinese hackers targeted Whitehall.” *The Guardian*. Guardian News and Media Limited, 5 September 2007. Web. 10 September 2010. <<http://www.guardian.co.uk/uk/2007/sep/05/topstories3.politics>>.

<sup>48</sup> *Idem*.

<sup>49</sup> Gaudin, Sharon. “Government informant is called kingpin of largest U.S. data breaches.” *Computerworld*. Computerworld Inc., 18 August 2009. Web. 10 September 2010. <[http://www.computerworld.com/s/article/9136787/Government\\_informant\\_is\\_called\\_kingpin\\_of\\_largest\\_U.S.\\_data\\_breaches](http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches)>.

<sup>50</sup> *Idem*.

<sup>51</sup> *Idem*.

third time.<sup>52</sup> Gonzalez's first two indictments occurred in 2008 for the cybertheft of credit card numbers.<sup>53</sup> The first indictment charged Gonzalez with the theft of credit card numbers from the online systems of Dave & Busters, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, and DSW.<sup>54</sup> The second indictment charged Gonzalez with the cybertheft of credit card numbers from TJX Companies Inc. – the owner of retail chains such as T.J.Maxx, Marshall's, and Bob's Stores.<sup>55</sup> At the time of this massive online identity theft in 2005, 2006, and 2007, Gonzalez stole 45.6 million credit card numbers.<sup>56</sup> This was considered the largest cyber identity theft ever, and few could imagine a larger scam may occur.<sup>57</sup>

January 2009 brought news that shook the cyberworld: the numbers of the TJX breach had been surpassed.<sup>58</sup> Heartland Payment Systems Inc. is a company that provides credit and debit card processing systems.<sup>59</sup> The corporation reluctantly admitted, after news of the breach broke, that malicious software was downloaded onto the supposedly-secure systems allowing hackers to access credit card numbers and other personal information.<sup>60</sup> Credit card companies Visa and MasterCard originally alerted Heartland that a possible breach had been detected and Heartland responded by announcing that a "widespread global cyberfraud operation" could be possible.<sup>61</sup> However, neither Heartland nor the credit card companies realized at the time how severe the breach actually was. On 17 August 2009, Albert Gonzalez was indicted, along with two Russian hackers, for the cybertheft of more than 130 million credit card numbers from Heartland in the largest case of cyber identity theft reported.<sup>62</sup> In addition to the credit card numbers, Gonzalez gained access to personal identification

---

<sup>52</sup> Idem.

<sup>53</sup> Idem.

<sup>54</sup> Idem.

<sup>55</sup> Vijayan, Jaikumar. "TJX data breach: At 45.6M card numbers, it's the biggest ever." *Computerworld*. Computerworld Inc., 29 March 2007. Web. 11 September 2010.  
<[http://www.computerworld.com/s/article/9014782/TJX\\_data\\_breach\\_At\\_45.6M\\_card\\_numbers\\_it\\_s\\_the\\_biggest\\_ever](http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever)>.

<sup>56</sup> Idem.

<sup>57</sup> Gaudin, Sharon. "Government informant is called kingpin of largest U.S. data breaches." *Computerworld*. Computerworld Inc., 18 August 2009. Web. 10 September 2010.  
<[http://www.computerworld.com/s/article/9136787/Government\\_informant\\_is\\_called\\_kingpin\\_of\\_largest\\_U.S.\\_data\\_breaches](http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches)>.

<sup>58</sup> Vijayan, Jaikumar. "Heartland data breach could be bigger than TJX's." *Computerworld*. Computerworld Inc., 20 January 2009. Web. 11 September 2010.  
<[http://www.computerworld.com/s/article/9126379/Heartland\\_data\\_breach\\_could\\_be\\_bigger\\_than\\_TJX\\_s](http://www.computerworld.com/s/article/9126379/Heartland_data_breach_could_be_bigger_than_TJX_s)>.

<sup>59</sup> Idem.

<sup>60</sup> Idem.

<sup>61</sup> Idem.

<sup>62</sup> Gaudin, Sharon. "Government informant is called kingpin of largest U.S. data breaches." *Computerworld*.

information from five companies including Heartland, 7-Eleven Inc., and Hannaford Bros. Co.<sup>63</sup> Since reporting the breach, Heartland has spent at least \$12.6 million to cover the costs incurred by the breach, including an estimated \$7 million fine imposed by MasterCard.<sup>64</sup> Considered “the Bernie Madoff of online data theft,”<sup>65</sup> Gonzalez has been described by the United Nations as “the single most prolific identity thief in ... history.”<sup>66</sup> U.S. District Court Judge Douglas P. Woodlock sentenced Gonzalez in March 2010 to twenty years in prison for the Heartland breach after he pled guilty.<sup>67</sup> This twenty year sentence will run concurrent to two his two other twenty year sentences for the Dave & Busters and TJX breaches.<sup>68</sup> The twenty eight year old stated “I am guilty of these crimes ... I accept full responsibility for these actions. I understand that the road to redemption is going to be long for me.”<sup>69</sup> Without parole, the world’s most accomplished individual cyber identity thief will be released from prison in 2030.

AT&T and Google have each received significant attention recently for breaches in their secure systems. Mid-2010 introduced a new wave of cyberattacks through the new iPad from Apple. A breach in the system allowed hackers to gain access to the e-mail addresses of iPad owners.<sup>70</sup> The website Gawker identified the hacking company Goatse Security as the perpetrator that stole personal information from 114,000 iPad owners, including high ranking officials in the United States government.<sup>71</sup> AT&T claimed to have fixed the breach as soon as it was discovered<sup>72</sup> and assured

---

Computerworld Inc., 18 August 2009. Web. 10 September 2010.

<[http://www.computerworld.com/s/article/9136787/Government\\_informant\\_is\\_called\\_kingpin\\_of\\_largest\\_U.S.\\_data\\_breaches](http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches)>.

<sup>63</sup> Idem.

<sup>64</sup> Vijayan, Jaikumar. “Heartland Breach Cost \$12.6 Million and Counting.” *Business Center*. PCWorld Communications Inc., 18 May 2009. Web. 11 September 2010.

<[http://www.peworld.com/businesscenter/article/165056/heartland\\_breach\\_cost\\_126\\_million\\_and\\_counting.html](http://www.peworld.com/businesscenter/article/165056/heartland_breach_cost_126_million_and_counting.html)>.

<sup>65</sup> Gaudin, Sharon. “Government informant is called kingpin of largest U.S. data breaches.” *Computerworld*.

Computerworld Inc., 18 August 2009. Web. 10 September 2010.

<[http://www.computerworld.com/s/article/9136787/Government\\_informant\\_is\\_called\\_kingpin\\_of\\_largest\\_U.S.\\_data\\_breaches](http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches)>.

<sup>66</sup> “Cybercrime.” *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. New York: United Nations Publications, 2010. 201-218. Print. <<http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>>.

<sup>67</sup> Weil, Nancy. “Hacker Gonzalez gets 20 years for Heartland breach.” *Network World*. Network World, Inc., 26 March 2010. Web 11 September 2010. <<http://www.networkworld.com/news/2010/032610-hacker-gonzalez-gets-20-years.html>>.

<sup>68</sup> Idem.

<sup>69</sup> Idem.

<sup>70</sup> Sydell, Laura. “Breach Exposed iPad Users’ E-Mail Addresses.” *NPR*. NPR, 9 June 2010. Web. 14 June 2010.

<<http://www.npr.org/templates/story/story.php?storyId=127698548>>.

<sup>71</sup> Idem.

<sup>72</sup> Idem.

patrons that passwords, e-mail contents, and other personal account details were never stolen.<sup>73</sup> Global search engine Google came under investigation from Privacy International (PI) as well as police forces in Australia, France, Germany, and the United Kingdom.<sup>74,75</sup> The StreetView software published by Google was identified as containing a program to collect data on unsecured Wi-Fi networks.<sup>76</sup> PI believes Google intentionally included the program to collect the data; if the allegations made by PI are correct, Google has transgressed interception laws in at least thirty countries.<sup>77</sup> Google claims the inclusion was accidental and attributes the situation to “systematic failure” claiming “a failure of communication between and within teams.”<sup>78</sup> In response to these, and other, breaches, countries are beginning to place a larger emphasis on cybersecurity. The United States Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau, for example, has declared cybersecurity a “high priority.”<sup>79</sup>

2008 marked Operation Centurion: a major Australian investigation into a child pornography ring.<sup>80</sup> The investigation began when hackers posted ninety-nine explicit images on a legitimate European website.<sup>81</sup> Within 76 hours, the images were deleted but an extraordinary 12 million views were already recorded for the website from almost 150,000 computers in about 170 countries.<sup>82</sup> The Australian authorities discovered a shockingly high number of Australian citizens downloaded the images onto their computers and discovered the postings originated in Australia.<sup>83</sup> The Australian police have arrested ninety individuals in connection with the child pornography ring, including teachers and community officials.<sup>84</sup> A similar case, though less visible on the international scale, occurred in 2009.<sup>85</sup>

---

<sup>73</sup> Hall, Jessica. “AT&T to work with law enforcement on iPad breach.” *Reuters*. Ed. Anshuman Daga. Thomson Reuters, 13 June 2010. Web. 14 June 2010. <<http://www.reuters.com/article/technologyNews/idUSTRE65D0GI20100614>>.

<sup>74</sup> “Google under investigation by Met Police.” *News: Technology*. BBC, 23 June 2010. Web. 23 June 2010. <<http://www.bbc.co.uk/news/10391096>>.

<sup>75</sup> “Google accused of criminal intent over StreetView data.” *News: Technology*. BBC, 9 June 2010. Web. 14 June 2010. <<http://www.bbc.co.uk/news/10278068>>. “Google under investigation by Met Police.” *News: Technology*. BBC, 23 June 2010. Web. 23 June 2010. <<http://www.bbc.co.uk/news/10391096>>.

<sup>76</sup> *Idem*.

<sup>77</sup> *Idem*.

<sup>78</sup> *Idem*.

<sup>79</sup> Poirier, John. “U.S. steps up Web security focus after iPad breach.” *Reuters*. Ed. John Wallace. Thomson Reuters, 11 June 2010. Web. 14 June 2010. <<http://www.reuters.com/article/idUSTRE65A4GH20100611>>.

<sup>80</sup> Allard, Tom. “Child sex abuse: Centurion’s shocking fact file.” *The Age*. Fairfax Media, 5 June 2008. Web. 11 September 2010. <<http://www.theage.com.au/national/child-sex-abuse-centurions-shocking-fact-file-20080605-2m4g.html>>.

<sup>81</sup> *Idem*.

<sup>82</sup> *Idem*.

<sup>83</sup> *Idem*.

<sup>84</sup> *Idem*.

<sup>85</sup> “Canada porn sweep nets 57 arrests.” *UPI.com*. United Press International, Inc., 26 March 2009. Web. 11 September

With the help of the National Child Exploitation Coordination Center, thirty Canadian police agencies arrested fifty-seven individuals on charges of “sexual assault, sexual interference and possessing, making and distributing child pornography.”<sup>86</sup> Child pornography websites aren’t limited to national groups of cybercriminals, however. A 2007 Austrian investigation led to over 2500 suspects – ranging in age from 17 to 69 – in 77 countries.<sup>87</sup> In one of the biggest strikes against child pornography, Austria identified a global porn website operated by an Austrian company.<sup>88</sup> The website itself is Russian, with videos uploaded from Eastern European countries and from the United Kingdom.<sup>89</sup> The investigation led to suspects in Britain, Austria, the United States, Germany, and France and to the confiscation of at least eight terabytes of illicit materials.<sup>90</sup>

States themselves have been the primary victims of recent relentless cyberattacks. The United States claims cyberattacks on military networks have increased exponentially over the last decade.<sup>91</sup> Estimates place the number of probings of military and civilian networks at several thousand times each day.<sup>92</sup> US officials claim the majority of cyberattacks originate in the People’s Republic of China.<sup>93</sup> Chinese officials vehemently deny the claims and argue that China has never organized hackers or developed forces for cyberattacks.<sup>94</sup> The Irish Central Applications Office (CAO) experienced a several day long DDoS attack in August 2010.<sup>95</sup> The website was inaccessible for at least three day and the severity of the attack forced officials to issue new passwords to 22,000 users.<sup>96</sup> The Gardaí (the Irish police force) claimed the motives behind the attack were unknown and the attack was traced to fake IP addresses: an abrupt end to the trail.<sup>97</sup>

---

2010. <[http://www.upi.com/Top\\_News/2009/03/26/Canada-porn-sweep-nets-57-arrests/UPI-30211238097445/](http://www.upi.com/Top_News/2009/03/26/Canada-porn-sweep-nets-57-arrests/UPI-30211238097445/)>.

<sup>86</sup> Idem.

<sup>87</sup> “Austria uncovers global porn site.” *The Times*. Times Newspapers Ltd., 8 February 2007. Web. 11 September 2010. <<http://www.timesonline.co.uk/tol/news/world/europe/article1350449.ece>>.

<sup>88</sup> Idem.

<sup>89</sup> Idem.

<sup>90</sup> Idem.

<sup>91</sup> Ide, William. “Cyber Attacks Against US Military Computers Increase Sharply.” *VOANews*. Voice of America, 26 August 2010. Web. 11 September 2010. <<http://www.voanews.com/english/news/usa/Cyber-Attacks-Againts-US-Military-Computers-Increase-Sharply-101613048.html>>.

<sup>92</sup> Idem.

<sup>93</sup> Idem.

<sup>94</sup> Liang Jun. “China denies launching cyber attack on US.” *People’s Daily Online*. People’s Daily Online, 18 August 2010. Web. 11 September 2010. <<http://english.peopledaily.com.cn/90001/90776/90883/7108678.html>>.

<sup>95</sup> Carroll, Steve. “Gardaí investigate CAO cyber attacks.” *irishtimes.com*. irishtimes.com, 27 August 2010. Web. 11 September 2010. <<http://www.irishtimes.com/newspaper/breaking/2010/0827/breaking50.html>>.

<sup>96</sup> Idem.

<sup>97</sup> Idem.

The Republic of Korea (ROK) has experienced a plethora of cyberattacks within the last eight months alone. June 2010 exhibited DDoS attacks on several government websites within two weeks.<sup>98</sup> The Ministry of Public Administration and Security announced it blocked access to the government websites from over two hundred computers located outside of the ROK, mostly in China.<sup>99</sup> Government officials claim the Democratic People's Republic of Korea (DPRK) is responsible for this attack, as well as crippling attacks on both the ROK and the USA governments in 2009.<sup>100</sup> ROK government officials explain the DPRK – which is still technically at war with the ROK due to the lack of a peace treaty after the Korean War in the 1960s – has a cyberwarfare unit with the purpose of hacking into foreign government networks.<sup>101</sup> Attacks with a more malicious intent were carried out on ROK servers between January and March 2010.<sup>102</sup> Hackers accessed the computers of over a dozen servicemen and stole 1,715 classified military documents, including war plans against the DPRK.<sup>103</sup> The ROK government has also identified seventy one individuals who knowingly leaked military secrets between January and June 2010, as well as fifty nine individuals who mistakenly leaked sensitive information.<sup>104</sup> While the governments of the ROK and the United States have experienced the greatest number of attacks on governments, China is still the most dangerous state in terms of cyberattacks: Chinese citizens are affected by more cyberattacks than citizens in any other country.<sup>105</sup>

The United Nations (UN) has been hesitant to engage in the prevention of and protection against cybercrime. When addressing the issue of international crime, the UN primarily focuses on organized crime. The UN Office on Drugs and Crime (UNODC) argues that the most common cybercrimes – identity theft, intellectual property violation, and the dissemination of child pornography – are crimes commonly performed by individuals or small groups.<sup>106</sup> Cyberspace allows criminals from across the world to meet and communicate instantly and anonymously, but the profits for these crimes are often

---

<sup>98</sup> “New cyberattacks in SKorea; sites suffer no damage.” *KSTP TV*. The Associated Press, 13 June 2010. Web. 16 June 2010. <<http://kstp.com/news/stories/S1023779.shtml?cat=159>>.

<sup>99</sup> *Idem*.

<sup>100</sup> *Idem*.

<sup>101</sup> *Idem*.

<sup>102</sup> Hur Jin and Moon Gwang-lip. “Cyberattacks get away with 1,715 military secrets.” *JoongAng Daily*. JoongAng Ilbo, 20 August 2010. Web. 11 September 2010. <<http://joongangdaily.joins.com/article/view.asp?aid=2924908>>.

<sup>103</sup> *Idem*.

<sup>104</sup> *Idem*.

<sup>105</sup> Greene, Tim. “Quiz: Separate cyber security fact from fiction.” *Network World*. Network World Inc., 15 October 2009. Web. 7 September 2010. <<http://www.networkworld.com/slideshows/2009/101609-cybersecurity-quiz.html#>>.

<sup>106</sup> “Cybercrime.” *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. New York: United Nations Publications, 2010. 201-218. Print. <<http://www.unodc.org/unodc/en/data-and-analysis/tocta-2010.html>>.

distributed amongst the primary individuals and not organized criminal groups.<sup>107</sup> Furthermore, the line between an international cybercrime and a national cybercrime is very faint and the question becomes: by entering into the world of cybersecurity does the UN affect the sovereignty of its Member States in the realms of communications and law enforcement?

### *Directive*

The Age of the Internet has introduced many benefits to the modern era: an increased availability of knowledge and resources, instant global communication, paperless files, remote shopping, digital spectacles never thought possible, and more. But the dawn of the internet has also introduced many dangers: increased opportunities for identity theft, a plethora of information for stalkers and other criminals, malware, spyware, spam, and thousands of other dangers. Broadly stated, the Age of the Internet has allowed for a new era of crime: an era of cybercrime.

Most individuals are careless with the information they place on the internet and have few qualms with whom they share private details. A teenager in the Russian Federation can easily rob the identity of a middle-aged woman in Brazil. A pedophile can easily become friends with every underage child in a five mile radius and convince them to meet. And a well-connected hacker could collapse a government, and through the government an entire country.

The facets of cybercrime are limitless: identity theft, illicit downloads, hacking, phishing, sharing child pornography, and millions of other crimes. And because the World Wide Web is global, the crimes reach across borders and blur jurisdictional lines. Delegates should first decide who has jurisdiction over cybercrimes: states, international institutions, or a mixture of both. If the international system, how are the differences in states' legal statutes reconciled? Or are the legal statutes of certain states accepted while those from other states are ignored?

One of the biggest dangers of the Internet Age is cyberterrorism. Often performed as part of an organized crime syndicate, cyberterrorism attempts to steal government secrets, bypass government security, and even shut down a government. This poses a major threat to individual states as well as the international system. Delegates should focus part of the discussion on how to prevent against and

---

<sup>107</sup> Idem.

prosecute cyberterrorism. But when a state performs actions of cyberterrorism against another state, the crime becomes cyberwar. Delegates should discuss whether cyberwar is legal, and if it is not how cyberwar should be prevented and prosecuted.

Finally, delegates will examine those crimes often committed by individuals: identity theft, phishing, malware, child pornography, and more. Delegates should once again question who has jurisdictional authority over these cybercrimes when they are perpetrated across borders. How are these crimes prevented? Can they be prevented? Delegates should be able to discuss basic concepts of cybersecurity and should identify the means by which states and the international system can protect against those cybercrimes that reach across borders.

The overlying question of this debate is: how do states and the international system prevent against and prosecute cybercrimes, especially cyberterrorism? Can states solve these issues on their own or do states inherently, by accepting the World Wide Web, surrender some sovereignty to a global phenomenon?