2011

Cyber Threats: Cyber Crime, Cyber Terror, and Cyber Warfare -- Transnational Risk in the Internet's Global Commons

David J Rodziewicz, J.D.

Cyber Threats: Cyber Crime, Cyber Terror, and Cyber Warfare

Transnational Risk in the Internet's Global Commons

By David J. Rodziewicz[1]

I Introduction

Suburban Atlanta, GA: It had been a long week of travel and meetings and Bill was ready to get home. The limo driver was waiting in baggage claim, just as arranged. Now, just a short ride from the airport, he was not surprised to see his wife Sally's number pop up on the cell phone en route. "Hello honey, I'm about ten minutes out," he answered. Sally cut him off short, "Why didn't you tell me we were in money trouble and about all those other credit cards?" Both the question and Sally's tone woke Bill up. "What are you talking about?" he asked. Sally continued, "The grocery store declined my AMEX and Visa cards. When I came home I called the bank and they told me they froze all of our credit card accounts. They said we owe a hundred fifty-five thousand dollars on three Visa accounts alone. Bill, I didn't know we had all those cards. Honey, what's happening?" The driver was just pulling into the driveway; Bill said, "Honey, we've never been late on a single bill; I don't know what you're talking about but I intend to find out." The driver turned to Bill and told him that he'd have to pay cash since his card was just declined.

San Jose, CA: The server farm failed for the third time this week taking down the sales

[1] David Rodziewicz is the Managing Director of TransformationArts LLC and a former KPMG Consulting Partner. He started his career as an information systems analyst with LTV Aerospace and Defense, Missiles and Electronics Division. Mr. Rodziewicz received his J.D. from Barry University's Andreas School of Law.

website and the boss was furious. It was the worst possible time - the television ads had just run offering a "buy-one-get-one free when you refer a friend" promotion. Now customers were getting an error code instead of an order screen. No one was surprised when the boss scheduled a crisis meeting with the entire IT senior leadership team.

The meeting started pretty normally with Steve, the CEO, in his trademark blue t-shirt and running shoes. There were several new faces, all wearing suits, around Steve. His usual kickoff was to say, "Good morning smiling faces!" But not today. Steve looked down, somberly reading from a prepared sheet, "Yesterday at 4:30 p.m. local time, my office received a call demanding fifty million US dollars in exchange for a cessation of attacks on our servers. The caller had an Eastern European accent; his directions were specific. I contacted the FBI and requested their assistance in identifying the perpetrators. They will now make a brief statement and interview each of you privately. Do not discuss what you have heard in this room with anyone except the FBI." In this moment, the beloved culture of the company forever changed.

Washington, D.C.: It had already been a bad night and the morning was not looking better. Rain and fog outside and short tempers inside the briefing room, coffee not yet served. Last evening, ten states from Michigan to Maine were off the power grid. Millions were without electricity then and are now. Half a world away, negotiations had broken down between North Korea and others in the Six-Party talks surrounding nuclear weapons on the Korean peninsula. A videoconference from Singapore was about to begin. The ambassador started by saying that talks were stalled again but he had another more pressing concern. The Chinese representative to

the talks asked for a private meeting. During that meeting China's delegate asked whether it wouldn't be better for the US to work on their internal electricity problems and leave this small regional problem to them. The delegate also said that he heard there was a problem with our phones and radios so a courier may be a better way to reach him. Static abruptly replaced the ambassador's face on the screen. A knock on the briefing room door broke the tension a few minutes after the ambassador's last statement. "All communications - radio, satellite, and ULF (ultra low frequency), military and civilian to Asia-Pacific command are down, sir. No explanation." What was going on here?

* * * * * *

"New evils require new remedies . . . new sanctions to defend and vindicate the eternal principles of right and wrong."[2]

* * * * * *

II Background

The Internet has been cast as the greatest single force of connection between nations in the industrial age.[3] From its humble roots as a defense intelligence network experiment to today's ubiquitous infrastructure necessity, much has changed in thirty years.[4] Global connection through exchange of information, ideas, and commerce has been enabled at a

[2] THE TIMES, *11 Nazi Leaders To Be Hanged*, *Death Sentences At Nuremberg*, Oct. 2, 1946, *available at*: http://archive.timesonline.co.uk/tol/viewArticle.arc?articleId=ARCHIVE-The_Times-1946-10-02-04-001&pageId=ARCHIVE-The_Times-1946-10-02-04.
[3] THOMAS P.M. BARNETT, THE PENTAGON'S NEW MAP 121-54 (2004).
[4] *Id.*

staggering speed.[5] Entire markets, industries, and economies have risen to meet the demand of hungry consumers across the globe.[6]

In this rapid expansion, however, other darker aspects have emerged. Some countries, like China, North Korea, and Iran, have tried intensively to regulate their citizens' access to the Internet.[7] Other countries harbor non-state sponsored criminals and terrorists who launch Internet-based attacks world-wide from within their borders.[8] These darker aspects of the Internet as a Global Commons require targets of attack to formulate defenses.[9]

A. Threats To Individuals

Specific threats to individuals include identity theft, bank and credit card theft, electronic extortion,[10] and the emerging theft of health insurance information.[11] These crimes are possible without an Internet intersection. Yet, the speed and reach of the Internet enables a quantum increase in the expansion of these crimes against individuals.[12] Many of these crimes are violations of state law,[13] but some crimes crossing state lines and of specific subject matter are

[5] *Id.*
[6] *Id.*
[7] BARNETT, *Supra* note 3 at 121-54.
[8] *Id.*
[9] Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L.Rev. 1, 23- 42 (2009).
[10] This refers to eExtortion attacks, like the "Pornado" that torrents the target PC with a tornado of pornography, including child pornography. The perpetrator then notifies, or threatens to notify, law enforcement anonymously unless the target remits a ransom. *See* http://tcattorney.typepad.com/anticybersquatting_consum/2007/12/trademarks-cybe.html.
[11] FED. BUREAU OF INVESTIGATION, INTERNET CRIME REPORT, 3-10, 17-23 (2009), *available at* http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf. Another computer scam is described within -- the "Hit-man" scam as detailed in this report.
[12] *Id.*
[13] CA, NY, and FL statutes follow in Section IV- Analysis of Law, below.

subject to Federal statutes.[14]

According to a 2009 study by the Center For Strategic and International Studies (CSIS), eighty-nine percent of those surveyed were aware of and had experienced a virus or malware system infection.[15] Also in 2009, the Federal Bureau of Investigation (FBI) reported an over twenty two percent increase of complaints received in the FBI's Internet Crime Center.[16] Over 146,000[17] cases were referred for prosecution (local, state or federal); the total dollar loss reported was approximately $560 million, and the median dollar loss was $575.[18] The top five categories were "non-delivered merchandise and/or payment [ranking] 19.9%; identity theft, 14.1%; credit card fraud, 10.4%; auction fraud, 10.3%; and computer fraud (destruction/damage/vandalism of property), 7.9%."[19] Of the claims referred for prosecution, "the highest median dollar losses were found among investment fraud ($3,200), overpayment fraud ($2,500), and advance fee fraud ($1,500) complainants."[20] The profile of perpetrators varied from individuals, to organized criminal networks, to non-state sponsored terror organizations.[21]

B. Threats To Enterprises

---

[14] Federal statutes follow in Section IV- Analysis of Law, below.
[15] STEWART BAKER ET AL, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3-9 (2009), *available at* http://resources.mcafee.com/content/NACIPReport.
[16] *Supra* note 11.
[17] This number is *double* the previous year's referrals for prosecution.
[18] *Supra* note 11.
[19] *Id.*
[20] *Id.*
[21] *Id.*

Attacks upon enterprises represent a more serious economic and societal threat.[22] In a 2010 presentation by the authors of the CSIS international study above, sixty percent of those surveyed experienced theft-of-service Cyber attacks, thirty percent had already experienced DDoS attacks (two-thirds of those attacks impacted operations), and twenty percent experienced extortion-via-network attacks.[23] The survey compiled a median downtime cost of six point three million dollars per twenty-four hour period.[24]

As the complexity of an attack increases, so do resources needed to accomplish the attack.[25] Perpetrators of these larger-scale attacks vary from individuals, to organized criminal networks, to non-state sponsored terror organizations and to state sponsors, as well.[26]

Consider the events surrounding Google's withdrawal from China in early 2010.[27] Google launched a business unit to target China's growing middle class.[28] Demographically, Google's investment was brilliant - internationally, this is the largest group of tech-savvy consumers with demand growing at double-digit rates.[29] Google and the Chinese government

---

[22] *Supra* note 15.
[23] STEWART BAKER, ET AL., CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR, 3-24 (2010), *available at* http://csis.org/files/attachments/100128_mcafee_CSIS.pdf. Mr. Baker prepared this Powerpoint set for a series of presentations in support of his research. Slides contain some updated data and observations.
[24] *Id.*
[25] THOMAS P.M. BARNETT, GREAT POWERS: AMERICA AND THE WORLD AFTER BUSH 44 (2009).
[26] NAT'L SEC. COUNCIL, EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW (2009) *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; JAMES R. LANGEVIN ET AL, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY (2009), *available at* http://resources.mcafee.com/content/NACIPReport.
[27] Justine Lau, *A Brief History Of Google In China,* THE GUARDIAN, Jan. 13, 2010, *available at* http://www.ft.com/cms/s/0/faf86fbc-0009-11df-8626-00144feabdc0.html; THE ECONOMIST, *Google & China: Flowers For A Funeral*, Jan. 14, 2010, *available at* http://www.economist.com/displayStory.cfm?story_id=15270952.
[28] *Id.*
[29] *Id.*

negotiated an agreement whereby Google would block access to certain websites in exchange for access to this coveted market.[30] In September 2007, China finally unblocked access to Google's site, more than eighteen months after the agreement. Google encountered many obstacles and gained significant market growth until January 2010, when Google announced it was considering ending censorship of site per their agreement. Shortly afterward, Google reported a sophisticated system Cyber attack infiltrated its operations in China.[31]

In another example, September 2010 press accounts identified a sophisticated attack against industrial computers using software from Siemens Corporation.[32] Once introduced, this virus called "Stuxnet" causes industrial control software, as used in energy production in nuclear power plants, to fail.[33] This virus, however, is highly sophisticated in its capacity to target

---

[30] *Id.*

[31] *Id.* One could write a book about the conflict between this US business and the government of China. This story is particularly instructive for US businesses abroad: local laws and customs govern professional practice. Google's perspective may have been to attack the Asian Market (Chinese in particular) with zeal and fervor, and an expectation that the local government would be supportive of expansive growth of Internet connection for its citizens, just like home. The communist government of China, however, had other objectives distasteful to Google. These include censorship, espionage, commercial infiltration, and facilitation of theft of international intellectual property (IP). The rumor is that Google was infiltrated in China, had their source code impacted (the Holy Grail of Google's IP), and had nowhere to turn since the Chinese government was the perpetrator.

China's perspective is simply that, as a sovereign nation, their government sets and enforces laws regarding communication within and outbound communication outside its borders. How it implements that control is solely the concern of the Chinese government. If a foreign firm wishes access to the Chinese market, compliance with this rule set is not optional.

Here, the tension is epic. The resulting negotiations had Google pull back to Hong Kong, then offer to return to Google's offices on the mainland if certain conditions were met. As of October 2010, Google's Chinese business unit is in flux.

[32] THE ECONOMIST, *The Meaning Of Stuxnet*, Sept. 30, 2010, *available at* http://www.economist.com/research/articlesBySubject/displaystory.cfm?subjectid=348963&story_id=17147862; Tom Gjelten, *Stuxnet Computer Worm Has Vast Repercussions*, NPR.ORG, Oct. 10, 2010 *available at* http://www.npr.org/templates/story/story.php?storyId=130260413.

[33] *Id.*

specific computers.[34] The Stuxnet virus might infiltrate a non-target computer control system, detect that it is not an intended target, and do no harm.[35] The quantum difference in the level of function and efficacy of this virus ("like a missile") led industry watchers to look to a nation as the sponsoring developer.[36] Dozens of industrial control systems in Iran were targeted, particularly those related to Iran's nuclear development program, while many systems in Europe were infected but not harmed.[37] A related concern to releasing a virus of this sort is the risk that others might try to copy the approach used without achieving target accuracy.[38] Once opened, this Pandora's box could lay waste to industrial infrastructure internationally.[39]

In early 2010, the Institute for Analysis of Global Security (IAGS) released a report highlighting China's strategy, research, and success in infiltrating and interfering with computer assets of U.S. energy firms.[40] The report showed evidence of infiltration of critical infrastructure, including the U.S. electricity grid and major U.S. oil companies' computer systems.[41] Recent testimony related to Transocean's Deepwater Horizon platform disaster in the Gulf of Mexico indicated continuing operational problems with control computers on the

---

[34] *Id.*
[35] *Id.*
[36] *Id.* Israel is the leading candidate for creation of this "tool."
[37] *Id.* As of late December 2010, The Stuxnet virus was widely reported as still crippling Iran's nuclear program. *See* http://www.foxnews.com/scitech/2010/12/09/despite-iranian-claims-stuxnet-worm-causing-nuclear-havoc/.
[38] *Id.* The concern is that a poor copy could replicate and infect unintended collateral systems in a rapidly spiraling, uncontrolled manner. There is a strong analogy to an engineered human pathogen's transmission but instead of person to person, this transmission could occur over networks system to system.
[39] *Id.*
[40] Daniel Ventre, *China's Strategy for Information Warfare: A Focus on Energy*, INSTITUTE FOR ANALYSIS OF GLOBAL SECURITY (2010) *available at* http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361.
[41] *Id.*

platform for months.[42] These control computers were used to monitor the status of the drill and well operations "including high gas levels or a fire."[43] One wonders if the IAGS's prediction of direct action against U.S. domestic energy targets came true.[44]

Perpetrators of threats to enterprises vary from organized crime syndicates, to non-state sponsored actors, to state sponsored agencies.[45] As a Cyber attack grows in scale from a solo threat to an enterprise, to a critical infrastructure threat, then to a national security threat, distinctions between threat levels become murky.

C. Threats to Nations

In 2007, the country of Estonia was besieged by a Cyber attack.[46] This organized Cyber

[42] Gregg Keizer, *Tech Worker Testifies Of "Blue Screen Of Death" On Oil Rig's Computer*, COMPUTERWORLD, July 23, 2010, *available at* http://www.computerworld.com/s/article/9179595/Tech_worker_testifies_of_blue_screen_of_death_on_oil_rig_s_computer. Some in the media have declared this an act of industrial espionage before this testimony was complete. What is striking is the prescience of the report in combination with the high-level anecdotal information. Security threats to oil platform control software, at least, will be under international review soon. Perhaps we should have an industrial incidents early warning database, much like the one the CDC uses for reports of unusual disease patterns in emergency rooms around the country.

[43] *Id.*

[44] *Supra* note 40.

[45] *Supra* note 26. In December 2010, a new generation of Cyber attackers emerged. After WikiLeaks release of a few hundred intercepted U.S. classified documents and the arrest of WikiLeaks founder, Julian Assange, on unrelated charges, factions for and against WikiLeaks began to play out a Cyber-skirmish with threat of all out Cyber War. These skirmishes impacted major international financial institutions and merchants. *See* http://www.washingtonpost.com/wp-dyn/content/article/2010/12/13/AR2010121305309.html and http://www.guardian.co.uk/technology/2010/dec/12/amazon-uk-offline-christmas.

[46] THE ECONOMIST, *Cyberwar: War In The Fifth Domain*, July 1, 2010, *available at* http://www.economist.com/node/16478792?story_id=16478792. Estonia rapidly gained prominence with economic expansion and technology assimilation after the collapse of the Soviet Union. The Estonian government decided to use Internet technologies in building their nation-state. Estonia adopted web based technologies for many infrastructure aspects of their citizen's interaction with government services. Banks, brokerages, utilities, and telecommunication providers were also early adopters of Internet based technologies. Juxtaposed against budding pride in Estonian capabilities, Russians marooned by the fall of the Soviet Union became a repressed ethnic minority overnight. Imagine the stark change for the ethnic Russians in Estonia circa 1991, virtually immediately after the

attack was launched after the removal of a statue in a Russian war memorial and in concert with protests by Estonia's Russian ethnic minority.[47] For a period of approximately three weeks, servers from across the world flooded Estonian networks and servers in an organized Dedicated Denial of Service (DDoS) attack.[48] Servers accustomed to traffic levels of a few thousand hits per week received as many as 2,000 hits per second.[49] The targets of the attack were initially Estonian government and ruling political party servers.[50] The attacks spread to bank, business, media, and telecommunication servers.[51] In doing so, the attacker(s) disrupted commerce, communication, and transportation throughout the entire country of Estonia for a period of weeks.[52] This attack has been colloquially called, "*Web* War One."[53] Estonia, as a member of the North Atlantic Treaty Organization ("NATO"), looked west for advice and counsel during

---

fall: no currency, no authority, and nowhere to flee.

[47] *Id.* Fast forward to 2006 with Russia making a return to the International political and economic scene, now as an "energy" economy. Estonia's decision to join NATO had to be disconcerting to Russia. Ethnic Russians in Estonia finally gained the attention of Russian President, Vladimir Putin, when a Soviet-era war memorial was removed by the Estonian government. The first wave of Cyber attacks coincided with riots in Talinn, Estonia's capital city.

[48] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia,* THE GUARDIAN, May 17, 2007, P1; Steven Lee Myers, *E-stonia Accuses Russia of Computer Attacks*, N.Y. TIMES, May 18, 2007, *available at* http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?_r=1&scp=1&sq=%22E-stonia%22&st=cse. A Dedicated Denial of Service (DDoS) attack can be compared to either: a) a phone line that is flooded with millions of calls a minute, rendering the line useless, or b) a mailbox that receives thousands of pieces of junk mail per hour. The bogus calls or mail obscure a user's ability to a) receive calls and transact business, or b) respond to important inbound messages; hence, the "Denial of Service" name. To accomplish his task, an attacker needs: a) a target or set of targets, b) a group of machines, usually private network connected personal computers infected by a worm or virus, and c) a triggering mechanism like a specific date or broadcast of a centralized command. Evolution of this type of attack has been in the triggering and targeting mechanisms of the virus. Sophisticated attack software is not the work of mischievous teens in a basement. Rather, complex software requires significant resources, time, and planning; look to governments, organized crime, or well-funded non-State sponsors. In extreme attacks, as the Estonian event was, the flood of message traffic collapsed entire networks. Even in the U.S., a significant portion of military and government communications travel over public access Internet pathways. Imagine the impact of a simultaneous collapse of broadband communication, cellular communication, electronic commerce, and radio + Television communication. This was the plight of Estonian citizens for about three weeks in 2007.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *Supra* note 46.

the crisis; none was forthcoming.[54] The Russian government was suspected but never proven to be responsible.[55]

In 2008, Russia deployed an attack of this sort *in concert* with a physical military invasion of Georgia.[56] President Mikheil Saakashvili's government contended with jammed telecommunication, no Internet access or communication, and a lack of effective backup for critical military and civilian communication during this crisis.[57] With Russian tanks rolling across its borders, Georgia's military command and control was disadvantaged by "the fog of Cyberwar."[58] At the time of the attack, several Russian websites were soliciting like-minded individuals to download software to join the cyber attack against Georgia.[59] These sites also included "a handy list of target websites," and "kill" status of the targeted website.[60]

Northrop Grumman Corporation prepared an analysis of China's capability and history

---

[54] *Supra* note 48.
[55] *Id.*
[56] John Markoff, *Before The Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008, *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&scp=1&sq=%22Before%20The%20Gunfire%22&st=cse; THE ECONOMIST, *Marching Off To Cyberwar*, Dec. 4, 2008, *available at* http://www.economist.com/node/12673385.. Like the Estonian Cyber attack before it, Georgia's problems were preceded by a series of terse negotiations with Russia. The Cyber attack and the physical, kinetic, military attacks were nearly simultaneous. Georgia, however, learned from the Estonian attack. It is widely reported that Georgia moved its servers to international sites to flee attack. This movement caused concern about an attack on resources of another country unrelated to the initial Cyber conflict. This involvement of a neutral party happened again in late 2010 when factions opposing the mission of WikiLeaks began a Cyber attack on WikiLeaks' European servers. WikiLeaks quickly moved to U.S. based servers contracted from Amazon. Amazon cancelled their service agreement, "eEvicting" WikiLeaks, when Amazon's servers came under attack in the days following WikiLeaks' move.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*

of using Cyber attacks in reaction to perceived economic, political, or military threats.[61] The report highlights a greater probability that a Chinese Cyber attack directed at the U.S.A. would be a disruptive event rather than a direct attack on command and control.[62] The report also models how a low-tech data incursion could corrupt data causing degradation in the reliability of resupply for items like fuel and food.[63]

The former United States Director of National Intelligence, Admiral Dennis Blair, reported to the Senate Select Committee on Intelligence in his annual threat analysis in February 2010. His first several pages of remarks focused upon emerging Cyber threats.[64] Blair also reported on the status of the newly created Comprehensive National Cybersecurity Initiative (CNCI) designed to meet and mitigate threats from Cyber Crime, Terror and War.[65] Blair had notions of how this threat may be met, but revealed few deliverables.[66]

Cyber attacks that start as enterprise-targeted may become uncontained, and through the law of unintended consequences, expand in size to present a nation-threat.[67] Much like the release of a human pathogen, a computer virus "in the wild" has the potential to impact any

---

[61] STEVEN KREKEL, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION (2009), www.uscc.gov/.../NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.
[62] *Id.* at 23 to 29.
[63] *Id.*
[64] *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, *Before the Sen. Select Comm. on Intelligence*, Feb. 2, 2010 (remarks of Admiral Dennis C. Blair, Director of National Intelligence).
[65] *Id.*
[66] *Id.*
[67] *Supra* note 32.

security-compromised computer the virus encounters.[68]

This article will discuss Cyber based threats to individuals, to enterprises, and to nations from a U.S. centric perspective. We will also review sources of state and U.S. Federal law, and International enforcement approaches that are used to combat these activities and the tension between these laws and policies to promote Internet growth. We will discuss the Internet governance efforts of several international actors including the United Nations ("UN") and the International Corporation for the Assignment of Numbers and Names ("ICANN") whether functional, dysfunctional, or a mix of both.

III Problem Statement

A. Cyber Attacks In General

Cyber attacks are disruptive.[69] To individuals, enterprises, and nations, the disruption created by loss of data, denial of services, theft of resources, or defense of information consume time and effort.[70] In the Estonian and Georgian examples, the attacks scaled upwardly, stressing and disrupting resources citizen relied upon to go to work, take children to school, or call a relative on the phone.[71]

---

[68] *Id.*
[69] *Supra* notes 46, 48 & 56.
[70] *Id.*
[71] *Id.* Scaling is a term used by information systems professionals and others to describe the capability of a set of software to grow and expand across servers. Software is considered "highly scalable" if the mere addition of server and disk hardware, with no change to the underlying software is required. This growth or scaling in hardware resource is also called distribution. A "highly scalable" virus is highly dangerous when it has the capability to use distributed resources, like thousands or millions of infected computers in a DDoS attack.

Cyber attacks are costly.[72] Costs calculated by theft of information, loss of service, damage, or defensive strategies are immense.[73] Consider FBI statistics for individual claimed loss estimates of approx $560 million,[74] enterprise losses of six point three million dollars per day attacked,[75] and U.S. investment of millions in preparation for an unseen but tangible threat from cyberspace.[76] Cascading events can result in permanently lost revenue, like meals not served or flights not flown. While tougher to estimate, these losses are thought to be a multiple of the losses above.[77]

Cyber attacks can unpredictably grow to threaten critical infrastructure, impacting quality of life.[78] In the Estonian and Georgian examples, the rapid increase in infected computers attacking and the expansion of servers attacked resulted in a collapse of systems critical to basic infrastructure, like communication, electricity, and basic government services.[79] Common to both scenarios, and to domestic infrastructure in the United States, is a (growing) reliance on the Internet as the backbone for commerce, communication, and basic services.[80]

Cyber attacks differ from traditional conflicts in the use of non-kinetic weapons and the character of the attack itself.[81] Major Graham Todd pointed this out in his 2009 article about

---

[72] *Supra* note 23.
[73] *Id.*
[74] *Supra* note 11.
[75] *Supra* note 23.
[76] *Supra* note 26.
[77] *Supra* notes 11 and 26.
[78] *Supra* note 32.
[79] *Supra* notes 46, 48 & 56.
[80] *Id.*
[81] Graham H. Todd, *Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition*, 64 A.F. L.Rev. 65 (2009).

asymmetric warfare in cyberspace, specifically,

> I would add four more distinguishing factors between cyberspace threats and traditional or kinetic uses of force: (1) cyberspace attacks can be completed literally at the speed of light; (2) the results of some cyberspace attacks, whether intended or not, can be similar to those involving weapons of mass destruction [WMD]; (3) the cost of acquiring the equipment and expertise to conduct operations in cyberspace is *de minimis* in comparison to fielding conventional forces; and (4) attributing the attack to the responsible party and determining whether the attack was intentional or accidental is extremely difficult.[82]

So high speed, WMD-type impact, minimal cost, and difficulty in attributing blame or intention all generally characterize this type of potential attack.[83]

The increasing tide of Cyber attacks is unlikely to soon recede. As citizens and enterprises rely upon their governments for national security, so too will they rely upon their governments for security against Cyber attack.

B. Exploitation and Espionage Versus War

In the common practice of gathering information from other nations, intelligence operations do not generally rise to acts of war. Espionage and exploitation of resources, both human and electronic, are merely tools of the intelligence service's trade.

It does not follow that every Cyber attack is a potential act of war, according to former CIA and NSA Director, Michael Hayden.[84] Nations test the security of other nations in a variety

[82] *Id* at 68-69.
[83] *Id.*
[84] Tom Gjelten, *Extending The Law Of War To Cyberspace*, NPR.ORG, Sept. 22-23, 2010 *available at*

of ways, including signals and electronic intelligence where electronic voice or data streams are analyzed, or human intelligence where people interact with human targets for the purpose of gathering information.[85] These are examples of exploitation and espionage in the classic sense.[86] Cyber incursions intended to probe and challenge the security of other nations' military computers occur regularly.[87]

Defining the boundaries between espionage, exploitation, and outright hostilities in Cyber terms is more difficult.[88] If targeting of a specific asset is imprecise, or the method used is not closely contained,[89] unintended consequences of the initial act are probable.[90] One reason is that military computers frequently work with civilian networks and servers.[91] As Tom Gjelten reported in a recent National Public Radio (NPR) series on Cyber War:

> The civilian computer infrastructure would include the networks that control an air traffic control system or a water supply, for example. But distinguishing civilian and military cybertargets is not necessarily so simple.
>
> "Computers don't always have signs over them that say, 'I'm a military target' [or] 'I'm a civilian target,' " says Harvard's Goldsmith. "Also, the two things are intermixed. Ninety to 95 percent of U.S. military and intelligence communications travel over private networks."[92]

Simply put, an attack on one could result in an attack on the other.[93] Even when harmful intent is not at the basis of an act of espionage or exploitation, the unintended consequences of Cyber

---

http://www.npr.org/templates/story/story.php?storyId=130023318 and http://www.npr.org/templates/story/story.php?storyId=130052701.

[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Supra* note 32.
[90] *Supra* note 84.
[91] *Id.*
[92] *Id.*
[93] *Id.*

attacks can blur the distinction between espionage, exploitation, and war.[94] It is ironic that similar technology can be used in pinpointing a target, decreasing collateral damage, yet use of targeting software in a Cyber weapon can become uncontained, increasing collateral damage.

C. Definitions Of War And Context

The term "war" has a variety of uses in our language and culture. It is useful to examine the following definitions and their approaches in trying to identify the offensive boundaries.

The Merriam-Webster Dictionary provides two useful baseline definitions for war: "1) *a (1)* **:** a state of usually open and declared armed hostile conflict between states or nations. . . [and] 2) *a* **:** a state of hostility, conflict, or antagonism."[95] While these definitions are not technical, nor even very precise, the common usage of the term "war" has value to the evaluation of when Cyber attack is an act of war.

A brief review of United States armed conflict in the twentieth century illuminates the challenge in presenting a clear definition of war. In a United States Constitutional sense, war is an advanced state of hostilities declared by an act of Congress.[96] It has therefore been argued that, strictly speaking, World War Two (WWII) was the last war the United States joined.[97] Later conflicts in Korea, Vietnam, Bosnia, and Iraq were hostilities other than war, lacking a formal declaration, but including armed conflict nonetheless.[98]

---

[94] *Id.*
[95] Merriam-Webster Online Dictionary 2010, "war," http://www.merriam-webster.com/dictionary/war.
[96] U.S. Const. art. I, § 8, cl. 11.
[97] STEVEN DYCUS ET AL., NATIONAL SECURITY LAW 201- 318 (4th ed. 2007).
[98] *Id.*

After WWII, like-minded nations established the United Nations (U.N.) resulting in the UN Charter and subsequent resolutions.[99] U.N. Charter article two, paragraph four, states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[100] At the same time, the U.N. is realistic in acknowledging a right to self-defense in article 51, specifically:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security. [101]

Note the language of these articles refers to "threat or use of force" in the context of an "armed attack."[102] Note that international conventions are effective if the offending party is deterred by the threat of international sanction.[103] The U.N. is struggling to design and implement a rule set to manage threats like these.[104] Gaining international consensus is another matter entirely.

Law professor and retired U.S. Army JAG Colonel Lee Schinasi uses this working

---

[99] U.N. Charter Introductory Note.
[100] U.N. Charter art. 2, para. 4.
[101] *Id.* art. 51.
[102] *Id.*
[103] For an asymmetric, non-state sponsored threat, like Al Qaeda or the Taliban for example, these sanctions might sound like "STOP, or I'll yell STOP again!" There is some belief that the U.S. military force transition after the cold war has increased special operations forces by an order of magnitude in recognition of asymmetric threats. *See generally*, BARNETT, *Supra* note 25 (observing motivation for and scope of US military force transition).
[104] *Supra* note 64.

definition: "War can be defined as a series of events that constitute a threat to continuity of the government and lifestyle of the United States."[105] This notion, without reference to nations or arms, presents a clear updated alternative to traditional transnational definitions of war. The definition does not have a requirement for intent, a symmetric, or asymmetric enemy. Instead, this definition of war focuses upon the thing to be protected.

At a certain theoretical attack threshold, a country's national interests would clearly be at stake.[106] The response to that attack is governed under international law by the principle of proportionality.[107] Proportionality in practice has evolved into a balance between military operational necessity (i.e., the need to "get" a military target) and the likelihood of innocent civilian casualties (i.e., "collateral damage").[108] A legitimate and unanswered question is whether an armed response is justified upon a Cyber attack's perpetrator when the attack threatens a nation's interests.

Today, there is a gap in both international law and enforcement regimes regarding this novel use of technology.[109] It is within this gap that international organized crime syndicates, non-state sponsored terrorists, and outlier nations dwell.[110]

D. Tension Between "Unfettered Growth of The Internet" & State Sovereignty

---

[105] Quoting a lecture by Professor Lee A. Schinasi, Colonel U.S. Army JAG (retired), Jan. 12, 2010.
[106] *Supra* note 64.
[107] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, opened for signature 8 June 1977, 1125 U.N.T.S. 3 (entered into force December 7, 1978) ("Additional Protocol I").
[108] Hamutal Esther Shamash, *How Much is Too Much? An Examination of the Principle of Jus in Bello Proportionality*. 2 Israel Defense Forces L. Rev. 2-4 (2006) *available at* http://ssrn.com/abstract=908369.
[109] *Supra* note 64.
[110] *Id.*

Much like airport security after the 9/11 attacks on the U.S., there is a tension between freedom of Internet access and security related to that access. Congress articulated the policy of the United States government "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation," through statute.[111] But the unfettered market espoused therein provides the enabling access and opportunity with few limits for Cyber attack.

The difficult balance is between maintaining open access to Internet resources while providing sovereign protections expected by the citizens of a nation, like domestic and national security. This gap, created by the wish for openness of access, was exploited during the Estonian and Georgian Cyber attacks.[112] Both states transitioned critical infrastructure communication to the Internet for the benefit of commerce and their citizens.[113] Neither state had sovereign control of access or a method to discontinue a Cyber attack upon their critical infrastructure once started.[114]

An analogy to sovereign boundaries in cyberspace can be drawn to the evolution of law and international convention encompassing boundaries in air and space.[115] First, international conventions applying to air flight have developed throughout most of the twentieth century, controlling formerly unfettered access to air space.[116] Sovereignty of air space became the norm

[111] 47 U.S.C §230(b)(2) (2009).
[112] *Supra* notes 46, 48, & 56.
[113] *Id.*
[114] *Id.*
[115] *Supra* note 9.
[116] *Id.* at 23.

during World War One (WWI), when neutral countries refused over-flights of their territories.[117] International conventions matured over the next eighty years and have resulted in requirements for nationality and registration code to be displayed on the aircraft and validated by nation of origin upon request.[118] Additionally, countries cooperating in this agreement recognize the complete and exclusive right of a nation to the airspace above its territory.[119] As International Cyberspace law and convention develop, these two features of international air convention, verifiable national registration and recognition of right, might be effective components of an approach to protect the Internet's Global Commons.

Next, the law and convention of space offers potential insight.[120] Near the height of the Cold War, the Outer Space Treaty of 1967 was formed.[121] A central agreement of this treaty was that no nation could declare sovereignty ownership of outer space or celestial bodies.[122] This notion approximates the status quo of sovereign borders in Cyberspace with a significant exception.

Countries wishing to isolate or disconnect their citizens from free exchange in the Global Commons may control network access through censorship or other restriction, imposing *de facto* sovereign boundaries in Cyberspace.[123] Notably, China selectively censors content while

---

[117] *Id.* Note that an analogous condition emerged in the Georgian conflict, and later with WikiLeaks when these entities shifted their Internet servers under attack to neutral countries (providers).
[118] *Id.* at 24 (*quoting* The Convention on International Civil Aviation, December 7, 1944, 61 Stat. 1180).
[119] *Id.*
[120] *Id.* at 25-27.
[121] *Id. (quoting* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410).
[122] *Id.*
[123] *Supra* note 3 (Barnett speaks eloquently of the forces of disconnection in China, Iran, and North Korea as a

encouraging international commerce through a governmental series of filters.[124] The recent Nobel Peace Prize award to Liu Xiaobo was a stark contrast: the Chinese government attempted to prevent communication with Liu's wife, Liu Xia, by removing her computer, phone line and Internet connection shortly after the announcement. Nevertheless, she resorted to a satellite phone and Twitter to communicate with the world.[125] It is in this way that sovereignty in Cyberspace is a two-edged sword. Raising sovereign boundaries in Cyberspace to control an attack from outside a nation's borders might be regarded as legitimate. Isolationist nations, however, go so far as to regard Twitter and Google as offensive weapons of attack against their national security and censorship regimes, and claim strategies of counterattack as a legitimate response.[126]

E. Emerging Definition of Cyber War

In attempting to find a definition for Cyber War, no single source seems precisely on point. I propose we combine three insightful sources, each with a different facet, important to crafting an emerging definition of Cyber War.

Major Graham Todd suggests that the asymmetric threat of Cyber attack requires an

---

danger to global stability).
[124] *Supra* note 27.
[125] Steven Jiang, *China Blanks Nobel Peace Prize Searches*, CNN, Oct. 8, 2010, *available at* http://www.cnn.com/2010/WORLD/asiapcf/10/08/china.internet/. Thus "a threat to the continuity of the government and lifestyle" of a country under Professor Schinasi's definition (i.e., the thing to be protected) may mean one thing to a democracy such as the United States, and something quite different and much broader to an isolationist regime such as China or Iran.
[126] *Id.*; *Supra* note 84.

asymmetric definition in two parts.[127] First, the modalities of attack are labeled "Cyber weapons" defined as "[a]ny capability, device, or combination of capabilities and techniques, which if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system."[128] Next, Major Graham uses a notion of international conduct to define the occurrence of a Cyber attack.[129] "A cyberspace attack occurs when a state knowingly uses or knowingly acquiesces to an entity under its legal control or within its territory using a cyberspace weapon against the people or property of another state."[130] These linked definitions are useful because they define: a) the nature of Cyber threats as weapons, and b) when the use of Cyber weapons amounts to an attack.[131] This linkage is critical in the context of domestic and international law below.

Walter Sharp considers "scope, duration, and intensity" of attack as the key factors to be considered on a case-by-case basis.[132] By Sharp's definition, the Estonian scenario above would justify an armed response, for example, based on these factors.[133]

Professor Schinasi's definition of war above focuses more broadly on protection of government and lifestyle rather than granularly on people and property.[134] Focusing on the thing to be protected is an essential portion of an effective framework both for law and remediation of

[127] *Supra* note 82 at 81-93 (Todd Asymmetric warfare/Definition).
[128] *Id.* at 83.
[129] *Id.* at 87.
[130] *Id.*
[131] *Id.*
[132] WALTER G. SHARP, SR., CYBERSPACE AND THE USE OF FORCE 69 (1999). "What constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the law of armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances."
[133] *Id.*; Supra note 46, 48, & 56.
[134] *Supra* note 105.

risk.

Thus, I propose the following hybrid definition of Cyber War:

> A Cyber War occurs when a state knowingly uses or knowingly acquiesces to an entity under its legal control or within its territory using, a cyberspace weapon against the people or property of a target nation, with sufficient scope, duration, and intensity to constitute a threat to continuity of the government and lifestyle of the target nation.[135]

Given the context of this hybrid definition, we will examine the sources of domestic and international law that either give rise to meaningful, lawful enforcement or illuminate gaps in need of remediation.

IV Analysis of Law

Many methods employed in Cyber Crime are classified as state law offenses and some are federal offenses. More grave and organized Cyber attacks, while certainly in violation of state law, are subject to prosecution under federal statute as seen below. But national Cyber Crime laws have lagged behind technological development. Approximately fifty-five percent of those surveyed in the 2009 CSIS research study judged the laws of their nations inadequate to respond to Cyber attack.[136] Nations are implementing infrastructure to analyze and cope with these uncertain and often unseen threats.[137] Individuals and corporations look to the rule of law in their locales for solutions at the same time that those homelands are struggling with emerging

[135] *Supra* note 82, 132, & 105. Assembly and edit by the author of this article.
[136] *Supra* note 23 at 18.
[137] *Supra* note 64.

Internet threats themselves.[138]

A. Sample of State Law Directed at Cyber Crime

Individual states have taken different approaches to define Cyber Crime in their efforts to protect their citizens and corporations from Internet threat. California, for example, enacted statutes to address a broad range of offenses involving Cyber Crime. These offenses may be charged in a stand-alone manner but were intended to supplement the charging of other offenses. California's statutes define Cyber Crimes directly as a series of unlawful acts, where, for example, one:

> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> (3) Knowingly and without permission uses or causes to be used computer services.
>
> (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
>
> (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

[138] *Supra* note 23.

> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
>
> (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.[139]

Punishment for these offenses in California ranges from a misdemeanor violation with a small fine for a minimally impactful first offense to three years in prison and a ten thousand dollar fine. Aggravating factors include losses in excess of five thousand dollars, and injury, or a repeat offense.[140] California statutes also include offenses related to credit card and identity theft, for example, that may be charged in addition to the Cyber Crime.[141]

New York uses a property theft analogy in its approach to Cyber crime.[142] Using a similar definition of modalities of offense as California, the New York statutes graduate crimes from unauthorized use, to computer trespass, to computer tampering in the fourth through first degrees.[143] These statutes all have an intent requirement.[144] The language used resembles a property violation with dollar loss being the sole aggravating factor.[145] New York statutes also include offenses related to credit card and identity theft that may be charged in addition to the

[139] CAL. PENAL LAW § 502(c) (West 2010).
[140] *Id.*
[141] CAL. PENAL LAW § 530 (West 2010).
[142] N.Y. PENAL LAW § 156 (Consol. 2010).
[143] *Id.* § 156.05-.27.
[144] *Id.*
[145] *Id.*

Cyber Crime.[146]

Florida's approach enacts supplemental statutes specific to Cyber Crime.[147] Legislative intent included in the text of the "Computer-Related Crimes" statute focuses on specific acts "through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets. . . ."[148] Florida criminalizes a range of Cyber Crimes, specifically:

> (1) Whoever willfully, knowingly, and without authorization:
>
> (a) Accesses or causes to be accessed any computer, computer system, or computer network;
>
> (b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;
>
> (c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;
>
> (d) Destroys, injures, or damages any computer, computer system, or computer network; or
>
> (e) Introduces any computer contaminant into any computer, computer system, or computer network,
>
> commits an offense against computer users.[149]

[146] N.Y. PENAL LAW §§ 190.75-.86 (Consol. 2010).
[147] FLA. STAT. § 815 (2010).
[148] *Id.* § 815.02(3).
[149] *Id.* § 815.06.

Florida's statute includes a graduated approach to penalties.[150] Although misdemeanors are defined in this statute, offenses involving losses greater that five thousand dollars, or intent to defraud, or acts that impact public infrastructure are second-degree felonies.[151] A Cyber related crime that "endangers a human life" is a first-degree felony with a sentence of thirty years to life and a ten thousand dollar fine.[152] Florida statutes also include offenses related to credit card and identity theft, for example, that may be charged in addition to the Cyber-Related Crime.[153] Florida is progressive in that its Cyber Crime statute explicitly includes factors for protection of human life and infrastructure, and clearly articulates statutory jurisdiction if any computing asset in Florida is compromised or used in a Cyber-Related Crime.[154]

Applying these sample state statutes to our introductory scenarios produces variable results. In the first scenario in which a couple experiences identity theft, statutes in all three states would apply to the use of stolen credit card or identity information. California and Florida differ from New York as to how the use of a computer in the commission of the crime impacts the charge. California and Florida treat the use of a computer in the commission of the credit card or identity theft as a crime in itself. New York does not include a charge for an additional Cyber Crime unless something of tangible value is stolen or destroyed as a result of a computer incursion of some sort. In the second scenario in which a business experiences a threat of extortion, all three states' statutes provide chargeable offenses. Where a resulting computer

[150] *Id.*
[151] *Id.* Related specifically to infrastructure interruption, the statute reads "[i]nterrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service."
[152] *Id.*
[153] FLA. STAT. §§ 817.481, 817.568 (statutes related to credit card and identity theft).
[154] *Supra* note 147.

disruption "endangers a human life," Florida is most progressive by charging a first-degree felony with a penalty of thirty years to life. California has a minor escalation in penalty when an injury occurs but still grades the offense by total dollar loss. New York's statute on Cyber Crime does not link this factor to penalty and uses a (property) loss model for charging, where an escalation of loss escalates charges.

These state statutes have a common trait that is simultaneously a potential strength and weakness. The state must have access to the person or significant property of that person within the jurisdiction of the state in order to achieve the desired effect of deterrence through enforcement. Applied domestically against individuals within U.S. borders, these statutes may prove effective. But in an international context, these state offenses are merely potential predicate offenses to Federal charges.

B. U.S. Federal Law Framework For Cyber Crime and Cyber Terror

The framework of Federal statutes surrounding Cyber Crime and Cyber Terror is complex. Statutes pertain to a range of offenses from simple identity theft to complex, layered criminal conspiracies under the Racketeer Influenced and Corrupt Organizations Act (RICO).[155]

[155] 18 U.S.C. §§ 1028, 1028A, 1961-68 (2010). *See also* CAN-SPAM Act, 18 U.S.C. §1037 (2010) – useful in DDoS prosecutions where impacted machines send thousands of messages an hour to a target; (Good Old Fashioned) Wire Fraud Act, 18 U.S.C. §1343 (2010) – in "executing a scheme or artifice" has higher initial penalties – 20 years or 30 years for fraud involving financial institutions; Wiretap Act, 18 U.S.C. §2511 (2010) – including penalties for intercepting, disclosing or using a protected communication, monetary penalties are $250K for an individual, $500K for an enterprise per offense; and, Unlawful Access to Stored Communications Act, 18 U.S.C.. § 2701 (2010) – Requires: "a) Intentional access, b) without or in excess of authorization, c) a facility that provided an electronic communication service [like an Internet Service Provider], d) obtained, altered, or prevented authorized access to a communication in electronic storage, e)(felonies only) for commercial advantage, malicious destruction or damage, private commercial gain, or in furtherance of a criminal or tortious act."

Some of these statutes define offenses directly chargeable as violations of Federal law; some require predicate offenses, such as a Federal misdemeanor or felony, or a state felony.[156] In the scheme of Federal statutes possible for prosecuting Cyber Crime and Cyber Terror offenses, two statutes stand out as the workhorses within the Department of Justice (DOJ).[157]

1. The Computer Fraud And Abuse Act

This Act defines a wide scope of prohibited activities from Cyber Crime, to Cyber Terror, to eExtortion, and to attack on U.S. national security assets.[158] The Act possesses broad coverage of potential perpetrators from individuals, to organized crime networks, to non-state sponsored terror organizations.[159] The key prohibited behaviors are based on "unauthorized access" or "access exceeding authorization."[160] The Act has seven major sections with differing objectives and penalties, specifically:

1) Obtaining National Security Information § 1030(a)(1),

2) Compromising the Confidentiality of a Computer § 1030(a)(2),

3) Trespassing in a Government Computer § 1030(a)(3),

4) Accessing a Computer to Defraud & Obtain Value § 1030(a)(4),

---

[156] *Id.*
[157] The U.S. DOJ produced a website as a detailed guide to prosecution of Cyber Crime. *See* U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIME (2007), *available at* http://www.cybercrime.gov/ccmanual/ccmanual.pdf.
[158] 18 U.S.C. § 1030 (2010). *See also* 18 U.S.C. § 1029 (2010) (related to fraud in connection with other access devices and useful in prosecution of "phishing" scams).
[159] *Id.*
[160] *Id.*

5) Knowing Transmission and Intentional Damage § 1030(a)(5)(A)(i), Intentional Access and Reckless Damage § 1030(a)(5)(A)(ii), and Intentional Access and Damage § 1030(a)(5)(A)(iii),

6) Trafficking in Passwords § 1030(a)(6), and

7) Extortion Involving Threats to Damage Computer § 1030(a)(7). [161]

This complex act was given extra-territorial reach by the USA Patriot Act of 2001.[162] Perpetrators of any of these seven unlawful acts are subject to investigation and enforcement even if the acts originated outside U.S. borders or passed through a U.S. computer or network in furtherance of the act.[163]

Sections of this statute address our introductory scenarios nicely. In the first scenario in which a couple experiences identity theft, sections that apply are: Compromising the Confidentiality of a Computer § 1030(a)(2), in that credit information could have been stolen to enable the couple's lack of credit; Accessing a Computer to Defraud & Obtain Value § 1030(a)(4), if a virus or other technique was used to steal information; and possibly Trafficking in Passwords § 1030(a)(6), if a password was stolen and subsequently sold resulting in harm. In the second scenario in which a business experiences a threat of extortion, Extortion Involving Threats to Damage Computer § 1030(a)(7) would likely apply since the threat intended to extort money was sent in interstate commerce via a phone call, and the threat occurred after damage

[161] *Id.*
[162] *Supra* note 157 at 93. *See also* 18 U.S.C. § 1029(h) (2010).
[163] *Id.*

was caused to servers and revenues of the business. Our final scenario is trickier since the inferred purveyor of the threat is another nation. If the perpetrator was a non-state sponsored group or an organized crime network, however, Knowing Transmission and Intentional Damage § 1030(a)(5)(A)(i) could apply since computers were knowingly infected and damaged resulting in a threat to public safety, at least.

2. Acts of Terrorism Transcending National Boundaries

This Act is significant because of its definitional scope and transnational reach.[164] Offenses defined in subsection (1) contemplate serious bodily harm or death caused by a variety of methods of offenses across national boundaries.[165] The jurisdictional bases for offenses include acts that obstruct commerce resulting in harm, a definition broad enough to include Cyber Crime and Cyber Terror.[166] Penalties in subsection (c) range from ten years, to any term of years including life imprisonment, or to death, depending on the magnitude of the resulting offense.[167] Congress added explicit extraterritorial jurisdiction in subsection (e) of the statute over any threat, attempt, conspiracy or individuals acting as accessories after the fact.[168]

In evaluating the applicability of this statute to our initial scenarios, the second and third scenarios fit well. In the corporate threat (i.e., second) scenario, if the website services disrupted in some way endangered life and limb, subsections (a)(1)(b) and (a)(2) would apply. In the third

[164] 18 U.S.C. § 2332b (2010).
[165] *Id.* § 2332b(a)(1).
[166] *Id.* § 2332b(b)(1).
[167] *Id.* § 2332b(c).
[168] *Id.* § 2332b(e).

scenario, again assuming an organized crime or non-state sponsored threat, the same subsections would apply.

These two statutes, in concert with other Federal law, might potentially deter some forms of Cyber Crime and attack that state law could not. The extraterritorial *jurisdiction* provisions bring with them extraterritorial *enforcement* potential. The U.S. maintains extradition treaties with over one hundred countries.[169] Without deterrent enforcement potential, these statutes are merely creatures of domestic U.S. policy and wither against transnational threats.

C. International Attempts To Curb Cyber Terror and Cyber War

1. U.N. Attempts

The U.N. Charter has evolved since 1945 with advisory prohibitions against use of force by member countries.[170] Specific to Cyber Terror and Cyber War, the U.N. is struggling for both consensus and relevance. The U.N. Charter is built around participation by member nations.[171] Cyber Terror and Cyber War are not necessarily the creatures of nations; non-state sponsors, as discussed above, are common.[172] The U.N. invested a decade in trying to formulate a flexible, effective means to combat state sponsored and non-state sponsored forms of Cyber Terror and Cyber War.[173] These efforts ended in failure in April 2010 with the rejection of a proposed U.N.

[169] For a current list of countries with whom the U.S. has an extradition treaty, *see* http://www.state.gov/www/global/legal_affairs/tifindex.html.
[170] *Supra* notes 100 & 101.
[171] *Id.*
[172] *Supra* note 26.
[173] AGENCE FRANCE-PRESSE, *U.N. Chief Calls For Treaty To Prevent Cyber War*, Jan. 30, 2010 *available at*

treaty focused on remediation and enforcement activities related to those topics.[174] Part of the U.N.'s continuing challenge is an insistence upon use of a symmetric, nation-driven set of solutions to a rapidly growing asymmetric problem.

2. Council of Europe's (EC) Convention on Cybercrime

The U.S. Senate ratified the EC's Convention on Cybercrime in 2006.[175] The EC's approach has three key objectives: a) unifying enforcement regimes across signatories, b) providing a basis in law for each signatory to gather, preserve, and share evidence with other signatories, and c) speeding investigation, prosecution and remediation of offenses.[176] This model is effective because it focuses on tools and tactics, and removes international barriers to information sharing and speedy response.[177] To date, there are forty-seven signatory nations participating in this convention.[178] The U.S. Department of Justice maintains a web page dedicated to information surrounding U.S. adoption of and international participation in this

---

http://www.google.com/hostednews/afp/article/ALeqM5h8Uvk-jpSvCWT-bqYSg1Ws4I4yAA; Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, Apr. 12-19, 2010, *A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime*, U.N. Doc. A/CONF.213/IE/7 *available at* http://www.un.org/en/conf/crimecongress2010/; Greg Masters, *Global Cybercrime Treaty Rejected at U.N.*, SC MAGAZINE, Apr. 23, 2010 available at http://www.scmagazineus.com/global-cybercrime-treaty-rejected-at-un/article/168630/.

[174] *Id.*

[175] Council of Europe Convention on Cybercrime, Aug. 3, 2006, 2001 U.S.T. Lexis 155.

[176] *Id.*

[177] *Id.*

[178] *Id.*

treaty.[179]

D. Proposed Remediation Of Law, Structure, and Process

1. Timely Changes To Federal Law

Based on the current threats and wild-west atmosphere of Cyber attack, I propose Congress consider new, more stringent penalties for specific Cyber related offenses. First, Congress should apply a penalty from life imprisonment up to death, for Cyber Crimes causing serious bodily injury or death, requiring no predicate federal offense. Next, Congress should increase minimum sentences for intentional interference with infrastructure to fifty years for the first offense and life imprisonment thereafter. Additionally, Congress should consider removing existing penalties from companies assisting government in legitimate, lawful, yet emergent investigations and remediation efforts.

2. Restructure ICANN

The current model of international assignment of Internet names and numbers through ICANN is unsustainable. I propose an Internet substructure based on individual nations or groups of nations (EC, ASEAN, NATO perhaps). ICANN could then function as the arbiter over disputes between sub-networks. Implicit in this proposal is that a sub-network could temporarily close if under attack. This proposal is tempered by the knowledge that some isolationist regimes would choose unacceptably to run their domestic networks "closed" all the

[179] *See* http://www.justice.gov/criminal/cybercrime/COEFAQs.htm.

time. Additionally, international message traffic needs a spoof-proof message identifier, much like the identification numbers on the tail of aircraft. Upon transmission of a message, its identifier could be verified with its sub-network source (or ICANN), just as an aircraft's tail number can be instantly verified by its country of origin. If bogus or tagged as suspicious, a validation process could reroute, hold, or discard the targeted traffic, discouraging growth of DDoS attacks.

3. Business Process Requirements

A disproportionate amount of business servers and computers are used in DDoS attacks. While more help is needed from technology providers, businesses need to maintain their systems in a competent and timely manner. Congress enacts legislation today applying to telecommunication, trucking, and air cargo arising under constitutionally granted powers to regulate interstate commerce. Domestic and international network safety demands similar minimum security and safety standards. Congress should additionally consider some remedial legislation to encourage (and perhaps require) companies to keep computers and networks updated with current security software. If an organization's computers and servers are found to be used as part of a DDoS attack, and are not using current protective software, a financial penalty would ensue.

V. Conclusion

This topic encompasses a rapidly changing area of law, technology, and society. In the last six months of 2010, the Stuxnet virus appeared, the WikiLeaks' Cyber attacks occurred, a

Cyber War was threatened between factions supporting and opposing WikiLeaks release of classified U.S. intelligence and diplomatic documents, and a countless number of Cyber incursions of Chinese and Eastern European origin upon U.S. servers occurred. The acceleration of threats is unlikely to subside.

New threats and new modalities emerge monthly. Many of the modalities are decidedly low-tech. Emerging high-tech threats like Stuxnet, however, bear close scrutiny. Once an all-consuming network genie is out of the bottle, no amount of retrospective analysis or regret will contain it. Broad infrastructure changes and additional rules of law are required to address these threats. International cooperation parallel to post-World War II reconstruction is needed to identify and remediate the root causes of this threat.

Until new remedies and sanctions are fully implemented, we are all under the threat of these new evils. In this battle of right and wrong, our challenge is mobilization in the face of an emerging, gathering threat.

VI. Appendix

A. Select California Statutes

California Penal Law Section 502 (Cyber crimes)

(a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data. The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:
(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.
(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.
(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.
(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.
(6) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.
(7) "Supporting documentation" includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software.
(8) "Injury" means any alteration, deletion, damage, or destruction of a computer system,

computer network, computer program, or data caused by the access, or the denial of access to legitimate users of a computer system, network, or program.
(9) "Victim expenditure" means any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access.
(10) "Computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.
(11) "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, assigned through centralized Internet naming authorities, comprising a series of character strings separated by periods, with the rightmost character string specifying the top of the hierarchy.

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:
(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
(3) Knowingly and without permission uses or causes to be used computer services.
(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.
(9) Knowingly and without permission uses the Internet domain name of another individual,

corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

(d)
(1) Any person who violates any of the provisions of paragraph (1), (2), (4), or (5) of subdivision (c) is punishable by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.
(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows: (A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.
(3) Any person who violates paragraph (6) or (7) of subdivision (c) is punishable as follows: (A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000). (B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.
(4) Any person who violates paragraph (8) of subdivision (c) is punishable as follows: (A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment. (B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or in the state prison, or by both that fine and imprisonment.
(5) Any person who violates paragraph (9) of subdivision (c) is punishable as follows: (A) For a first violation that does not result in injury, an infraction punishable by a fine not one thousand dollars. (B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not

exceeding one year, or by both that fine and imprisonment.

(e)
(1) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access. For the purposes of actions authorized by this subdivision, the conduct of an unemancipated minor shall be imputed to the parent or legal guardian having control or custody of the minor, pursuant to the provisions of Section 1714.1 of the Civil Code.
(2) In any action brought pursuant to this subdivision the court may award reasonable attorney's fees.
(3) A community college, state university, or academic institution accredited in this state is required to include computer-related crimes as a specific violation of college or university student conduct policies and regulations that may subject a student to disciplinary sanctions up to and including dismissal from the academic institution. This paragraph shall not apply to the University of California unless the Board of Regents adopts a resolution to that effect.
(4) In any action brought pursuant to this subdivision for a willful violation of the provisions of subdivision (c), where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud, or malice as defined in subdivision (c) of Section 3294 of the Civil Code, the court may additionally award punitive or exemplary damages.
(5) No action may be brought pursuant to this subdivision unless it is initiated within three years of the date of the act complained of, or the date of the discovery of the damage, whichever is later.

(f) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction, nor shall it make illegal any employee labor relations activities that are within the scope and protection of state or federal labor laws.

(g) Any computer, computer system, computer network, or any software or data, owned by the defendant, that is used during the commission of any public offense described in subdivision (c) or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture, as specified in Section 502.01.

(h)
(1) Subdivision (c) does not apply to punish any acts which are committed by a person within the scope of his or her lawful employment. For purposes of this section, a person acts within the

scope of his or her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.
(2) Paragraph (3) of subdivision (c) does not apply to penalize any acts committed by a person acting outside of his or her lawful employment, provided that the employee's activities do not cause an injury, as defined in paragraph (8) of subdivision (b), to the employer or another, or provided that the value of supplies or computer services, as defined in paragraph (4) of subdivision (b), which are used does not exceed an accumulated total of two hundred fifty dollars ($250).

(i) No activity exempted from prosecution under paragraph (2) of subdivision (h) which incidentally violates paragraph (2), (4), or (7) of subdivision (c) shall be prosecuted under those paragraphs.

(j) For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

(k) In determining the terms and conditions applicable to a person convicted of a violation of this section the court shall consider the following:
(1) The court shall consider prohibitions on access to and use of computers.
(2) Except as otherwise required by law, the court shall consider alternate sentencing, including community service, if the defendant shows remorse and recognition of the wrongdoing, and an inclination not to repeat the offense.

California Penal Law Section 530.5 (Identity & Credit Card Data Theft)

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(b) In any case in which a person willfully obtains personal identifying information of another person, uses that information to commit a crime in addition to a violation of subdivision (a), and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

(c)
(1) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is

guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment.
(2) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and who has previously been convicted of a violation of this section, upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.
(3) Every person who, with the intent to defraud, acquires or retains possession of the personal identifying information, as defined in subdivision (b) of Section 530.55, of 10 or more other persons is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

(d)
(1) Every person who, with the intent to defraud, sells, transfers, or conveys the personal identifying information, as defined in subdivision (b) of Section 530.55, of another person is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.
(2) Every person who, with actual knowledge that the personal identifying information, as defined in subdivision (b) of Section 530.55, of a specific person will be used to commit a violation of subdivision (a), sells, transfers, or conveys that same personal identifying information is guilty of a public offense, and upon conviction therefor, shall be punished by a fine, by imprisonment in the state prison, or by both a fine and imprisonment.

(e) Every person who commits mail theft, as defined in Section 1708 of Title 18 of the United States Code, is guilty of a public offense, and upon conviction therefor shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment. Prosecution under this subdivision shall not limit or preclude prosecution under any other provision of law, including, but not limited to, subdivisions (a) to (c), inclusive, of this section.

(f) An interactive computer service or access software provider, as defined in subsection (f) of Section 230 of Title 47 of the United States Code, shall not be liable under this section unless the service or provider acquires, transfers, sells, conveys, or retains possession of personal information with the intent to defraud.

B. Select New York Statutes

N.Y. Penal Code, Article 156 (Cyber Crimes)

Section 156.00 Offenses involving computers; definition of terms.

The following definitions are applicable to this chapter except where different meanings are expressly specified:

1. "Computer" means a device or group of devices which, by manipulation of electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data.

2. "Computer program" is property and means an ordered set of data representing coded instructions or statements that, when executed by computer, cause the computer to process data or direct the computer to perform one or more computer operations or both and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

3. "Computer data" is property and means a representation of information, knowledge, facts, concepts or instructions which are being processed, or have been processed in a computer and may be in any form, including magnetic storage media, punched cards, or stored internally in the memory of the computer.

4. "Computer service" means any and all services provided by or through the facilities of any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another.

5. "Computer material" is property and means any computer data or computer program which:

(a) contains records of the medical history or medical treatment of an identified or readily identifiable individual or individuals. This term shall not apply to the gaining access to or duplication solely of the medical history or medical treatment records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(b) contains records maintained by the state or any political subdivision thereof or any governmental instrumentality within the state which contains any information concerning a person, as defined in subdivision seven of section 10.00 of this chapter, which because of name, number, symbol, mark or other identifier, can be used to identify the person and which is otherwise prohibited by law from being

disclosed. This term shall not apply to the gaining access to or duplication solely of records of a person by that person or by another specifically authorized by the person whose records are gained access to or duplicated; or

(c) is not and is not intended to be available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent and which accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.

6. "Uses a computer or computer service without authorization" means the use of a computer or computer service without the permission of, or in excess of the permission of, the owner or lessor or someone licensed or privileged by the owner or lessor after notice to that effect to the user of the computer or computer service has been given by:

(a) giving actual notice in writing or orally to the user; or

(b) prominently posting written notice adjacent to the computer being utilized by the user; or

(c) a notice that is displayed on, printed out on or announced by the computer being utilized by the user. Proof that the computer is programmed to automatically display, print or announce such notice or a notice prohibiting copying, reproduction or duplication shall be presumptive evidence that such notice was displayed, printed or announced.

7. "Felony" as used in this article means any felony defined in the laws of this state or any offense defined in the laws of any other jurisdiction for which a sentence to a term of imprisonment in excess of one year is authorized in this state.

Section 156.05 Unauthorized use of a computer.

A person is guilty of unauthorized use of a computer when he knowingly uses or causes to be used a computer or computer service without authorization and the computer utilized is equipped or programmed with any device or coding system, a function of which is to prevent the unauthorized use of said computer or computer system.

Unauthorized use of a computer is a class A misdemeanor.

Section 156.10 Computer trespass.

A person is guilty of computer trespass when he knowingly uses or

causes to be used a computer or computer service without authorization and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he thereby knowingly gains access to computer material.

Computer trespass is a class E felony.

Section 156.20 Computer tampering in the fourth degree.

A person is guilty of computer tampering in the fourth degree when he uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person.

Computer tampering in the fourth degree is a class A misdemeanor.

Section 156.25 Computer tampering in the third degree.

A person is guilty of computer tampering in the third degree when he commits the crime of computer tampering in the fourth degree and:

1. he does so with an intent to commit or attempt to commit or further the commission of any felony; or

2. he has been previously convicted of any crime under this article or subdivision eleven of section 165.15 of this chapter; or

3. he intentionally alters in any manner or destroys computer material; or

4. he intentionally alters in any manner or destroys computer data or a computer program so as to cause damages in an aggregate amount exceeding one thousand dollars.

Computer tampering in the third degree is a class E felony.

Section 156.26 Computer tampering in the second degree.

A person is guilty of computer tampering in the second degree when he commits the crime of computer tampering in the fourth degree and he intentionally alters in any manner or destroys computer data or a computer program so as to cause damages in an aggregate amount exceeding three thousand dollars.

Computer tampering in the second degree is a class D felony.

Section 156.27 Computer tampering in the first degree.

A person is guilty of computer tampering in the first degree when he commits the crime of computer tampering in the fourth degree and he intentionally alters in any manner or destroys computer data or a computer program so as to cause damages in an aggregate amount exceeding fifty thousand dollars.

Computer tampering in the first degree is a class C felony.

Section 156.30 Unlawful duplication of computer related material.

A person is guilty of unlawful duplication of computer related material when having no right to do so, he copies, reproduces or duplicates in any manner:

1. any computer data or computer program and thereby intentionally and wrongfully deprives or appropriates from an owner thereof an economic value or benefit in excess of two thousand five hundred dollars; or

2. any computer data or computer program with an intent to commit or attempt to commit or further the commission of any felony.

Unlawful duplication of computer related material is a class E felony.

Section 156.35 Criminal possession of computer related material.

A person is guilty of criminal possession of computer related material when having no right to do so, he knowingly possesses, in any form, any copy, reproduction or duplicate of any computer data or computer program which was copied, reproduced or duplicated in violation of section 156.30 of this article, with intent to benefit himself or a person other than an owner thereof.

Criminal possession of computer related material is a class E felony.

Section 156.50 Offenses involving computers; defenses.

In any prosecution:

1. under section 156.05 or 156.10 of this article, it shall be a defense that the defendant had reasonable grounds to believe that he had authorization to use the computer;

2. under section 156.20, 156.25, 156.26 or 156.27 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to alter in any manner or destroy the computer data or the computer program;

3. under section 156.30 of this article it shall be a defense that the defendant had reasonable grounds to believe that he had the right to copy, reproduce or duplicate in any manner the computer data or the

computer program.

N.Y. Penal Code, Article 190 (Credit Card & Identity Theft)

Section 190.75 Criminal use of an access device in the second degree.

A person is guilty of criminal use of an access device in the second degree when he knowingly uses an access device without consent of an owner thereof with intent to unlawfully obtain telecommunications services on behalf of himself or a third person. As used in this section, access device shall have the meaning set forth in subdivision seven-c of section 155.00 of this chapter. Criminal use of an access device in the second degree is a class A misdemeanor.

Section 190.76 Criminal use of an access device in the first degree.

A person is guilty of criminal use of an access device in the first degree when he knowingly uses an access device without consent of an owner thereof with intent to unlawfully obtain telecommunications services on behalf of himself or a third person, and so obtains such services with a value in excess of one thousand dollars. As used in this section, access device shall have the meaning set forth in subdivision seven-c of section 155.00 of this chapter. Criminal use of an access device in the first degree is a class E felony.

Section 190.77 Offenses involving theft of identity; definitions.

1. For the purposes of sections 190.78, 190.79 and 190.80 of this article "personal identifying information" means a person's name, address, telephone number, date of birth, driver's license number, social security number, place of employment, mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, taxpayer identification number, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or personal identification number, or any other name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person. ** NB Effective until November 1, 2008

** 1. For the purposes of sections 190.78, 190.79, 190.80 and 190.85 of this article "personal identifying information" means a person's name, address, telephone number, date of birth, driver's license number, social security number, place of employment, mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, taxpayer identification

number, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or personal identification number, or any other name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person. ** NB Effective November 1, 2008 until November 4, 2008

2. For the purposes of sections 190.78, 190.79, 190.80, 190.81, 190.82 and 190.83 of this article: a. "electronic signature" shall have the same meaning as defined in subdivision three of section three hundred two of the state technology law. b. "personal identification number" means any number or code which may be used alone or in conjunction with any other information to assume the identity of another person or access financial resources or credit of another person. * NB Effective until November 4, 2008

Section 190.77 Offenses involving theft of identity; definitions.

1. For the purposes of sections 190.78, 190.79, 190.80 and 190.80-a and 190.85 of this article "personal identifying information" means a person's name, address, telephone number, date of birth, driver's license number, social security number, place of employment, mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, taxpayer identification number, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or personal identification number, or any other name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person.

2. For the purposes of sections 190.78, 190.79, 190.80, 190.80-a, 190.81, 190.82 and 190.83 of this article: a. "electronic signature" shall have the same meaning as defined in subdivision three of section three hundred two of the state technology law. b. "personal identification number" means any number or code which may be used alone or in conjunction with any other information to assume the identity of another person or access financial resources or credit of another person. c. "member of the armed forces" shall mean a person in the military service of the United States or the military service of the state, including but not limited to, the armed forces of the United States, the army national guard, the air national guard, the New York naval militia, the New York guard, and such additional forces as may be created by the federal or state government as authorized by law. * NB Effective November 4, 2008

Section 190.78 Identity theft in the third degree.

A person is guilty of identity theft in the third degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby: 1. obtains goods, money, property or services or uses credit in the name of such other person or causes financial loss to such person or to another person or persons; or 2. commits a class A misdemeanor or higher level crime. Identity theft in the third degree is a class A misdemeanor.

Section 190.79 Identity theft in the second degree.

A person is guilty of identify theft in the second degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby: 1. obtains goods, money, property or services or uses credit in the name of such other person in an aggregate amount that exceeds five hundred dollars; or 2. causes financial loss to such person or to another person or persons in an aggregate amount that exceeds five hundred dollars; or 3. commits or attempts to commit a felony or acts as an accessory to the commission of a felony; or 4. commits the crime of identity theft in the third degree as defined in section 190.78 of this article and has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in this section, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter. Identity theft in the second degree is a class E felony.

Section 190.80 Identity theft in the first degree.

A person is guilty of identity theft in the first degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby:
1. obtains goods, money, property or services or uses credit in the name of such other person in an aggregate amount that exceeds two thousand dollars; or
2. causes financial loss to such person or to another person or persons in an aggregate amount that exceeds two thousand dollars; or
3. commits or attempts to commit a class D felony or higher level crime or acts as an accessory in the commission of a class D or higher level felony; or
4. commits the crime of identity theft in the second degree as defined in section 190.79 of this

article and has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in this section, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter. Identity theft in the first degree is a class D felony.

* Section 190.80-a Aggravated identity theft.

A person is guilty of aggravated identity theft when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and knows that such person is a member of the armed forces, and knows that such member is presently deployed outside of the continental United States and:
1. thereby obtains goods, money, property or services or uses credit in the name of such member of the armed forces in an aggregate amount that exceeds five hundred dollars; or
2. thereby causes financial loss to such member of the armed forces in an aggregate amount that exceeds five hundred dollars. Aggravated identity theft is a class D felony. * NB Effective November 4, 2008

Section 190.81 Unlawful possession of personal identification information in the third degree.

A person is guilty of unlawful possession of personal identification information in the third degree when he or she knowingly possesses a person`s financial services account number or code, savings account number or code, checking account number MICR code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother`s maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person knowing such information is intended to be used in furtherance of the commission of a crime defined in this chapter. Unlawful possession of personal identification information in the third degree is a class A misdemeanor.

Section 190.82 Unlawful possession of personal identification information in the second degree.

A person is guilty of unlawful possession of personal identification information in the second degree when he or she knowingly possesses two hundred fifty or more items of personal identification information of the following nature: a person`s financial services account number or code, savings account number or code, checking account number or code, brokerage account

number or code, credit card account number or code, debit card number or code, automated teller machine number or code, personal identification number, mother`s maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person knowing such information is intended to be used in furtherance of the commission of a crime defined in this chapter. Unlawful possession of personal identification information in the second degree is a class E felony.

Section 190.83 Unlawful possession of personal identification information in the first degree.

A person is guilty of unlawful possession of personal identification information in the first degree when he or she commits the crime of unlawful possession of personal identification information in the second degree and:
1. with intent to further the commission of identity theft in the second degree, he or she supervises more than three accomplices; or
** 2. he or she has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in this section, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter. ** NB Effective until November 1, 2008 **
2. he or she has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in this section, unlawful possession of a skimmer device in the second degree as defined in section 190.85, unlawful possession of a skimmer device in the first degree as defined in section 190.86, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter. ** NB Effective November 1, 2008 until November 4, 2008 Unlawful possession of personal identification information in the first degree is a class D felony.
* NB Effective until November 4, 2008

Section 190.84 Defenses.

In any prosecution for identity theft or unlawful possession of personal identification information

pursuant to this article, it shall be an affirmative defense that the person charged with the offense: 1. was under twenty-one years of age at the time of committing the offense and the person used or possessed the personal identifying or identification information of another solely for the purpose of purchasing alcohol; 2. was under eighteen years of age at the time of committing the offense and the person used or possessed the personal identifying or identification information of another solely for the purpose of purchasing tobacco products; or 3. used or possessed the personal identifying or identification information of another person solely for the purpose of misrepresenting the person`s age to gain access to a place the access to which is restricted based on age.

Section 190.85 Unlawful possession of a skimmer device in the second degree.

1. A person is guilty of unlawful possession of a skimmer device in the second degree when he or she possesses a skimmer device with the intent that such device be used in furtherance of the commission of the crime of identity theft or unlawful possession of personal identification information as defined in this article. 2. For purposes of this article, "skimmer device" means a device designed or adapted to obtain personal identifying information from a credit card, debit card, public benefit card, access card or device, or other card or device that contains personal identifying information.
* NB Effective November 1, 2008
Unlawful possession of a skimmer device in the second degree is a class A misdemeanor.
Section 190.86 Unlawful possession of a skimmer device in the first degree.

A person is guilty of unlawful possession of a skimmer device in the first degree when he or she commits the crime of unlawful possession of a skimmer device in the second degree and he or she has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in section 190.80, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, unlawful possession of a skimmer device in the second degree as defined in section 190.85, unlawful possession of a skimmer device in the first degree as defined in this section, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter.
* NB Effective November 1, 2008 Unlawful possession of a skimmer device in the first degree is a class E felony.

C. Select FL Statutes

815.06 Offenses against computer users.

(1) Whoever willfully, knowingly, and without authorization:

(a) Accesses or causes to be accessed any computer, computer system, or computer network;

(b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another;

(c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network;

(d) Destroys, injures, or damages any computer, computer system, or computer network; or

(e) Introduces any computer contaminant into any computer, computer system, or computer network,

commits an offense against computer users.

(2)

(a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Whoever violates subsection (1) and:

1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is $5,000 or greater;

2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or

3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service,

commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(4)

(a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages.

(b) In any action brought under this subsection, the court may award reasonable attorney's fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701-932.704.

(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.

(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

817.481 Credit cards; obtaining goods by use of false, expired, etc.; penalty.

(1) It shall be unlawful for any person knowingly to obtain or attempt to obtain credit, or to purchase or attempt to purchase any goods, property or service, by the use of any false, fictitious, counterfeit, or expired credit card, telephone number, credit number, or other credit device, or by the use of any credit card, telephone number, credit number, or other credit device of another without the authority of the person to whom such card, number or device was issued, or by the use of any credit card, telephone number, credit number, or other credit device in any case where such card, number or device has been revoked and notice of revocation has been given to the person to whom issued.
(2) It shall be unlawful for any person to avoid or attempt to avoid or to cause another to avoid payment of the lawful charges, in whole or in part, for any telephone or telegraph service or for the transmission of a message, signal or other communication by telephone or telegraph or over

telephone or telegraph facilities by the use of any fraudulent scheme, means or method, or any mechanical, electric, or electronic device.
(3)
(a) If the value of the property, goods, or services obtained or which are sought to be obtained in violation of this section is $300 or more, the offender shall be guilty of grand larceny.
(b) If the value of the property, goods, or services obtained or which are sought to be obtained in violation of this section is less than $300 the offender shall be guilty of petit larceny.

817.568 Criminal use of personal identification information.

(1) As used in this section, the term:

(a) "Access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument.

(b) "Authorization" means empowerment, permission, or competence to act.

(c) "Harass" means to engage in conduct directed at a specific person that is intended to cause substantial emotional distress to such person and serves no legitimate purpose. "Harass" does not mean to use personal identification information for accepted commercial purposes. The term does not include constitutionally protected conduct such as organized protests or the use of personal identification information for accepted commercial purposes.

(d) "Individual" means a single human being and does not mean a firm, association of individuals, corporation, partnership, joint venture, sole proprietorship, or any other entity.

(e) "Person" means a "person" as defined in s. 1.01(3).

(f) "Personal identification information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:

1. Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food assistance account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

3. Unique electronic identification number, address, or routing code;

4. Medical records;

5. Telecommunication identifying information or access device; or

6. Other number or information that can be used to access a person's financial resources.

(g) "Counterfeit or fictitious personal identification information" means any counterfeit, fictitious, or fabricated information in the similitude of the data outlined in paragraph (f) that, although not truthful or accurate, would in context lead a reasonably prudent person to credit its truthfulness and accuracy.

(2)

(a) Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual's consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Any person who willfully and without authorization fraudulently uses personal identification information concerning an individual without first obtaining that individual's consent commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $5,000 or more or if the person fraudulently uses the personal identification information of 10 or more individuals, but fewer than 20 individuals, without their consent. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a mandatory minimum sentence of 3 years' imprisonment.

(c) Any person who willfully and without authorization fraudulently uses personal identification information concerning an individual without first obtaining that individual's consent commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $50,000 or more or if the person fraudulently uses the personal identification information of 20 or more individuals, but fewer than 30 individuals, without their consent. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a mandatory minimum sentence of 5 years' imprisonment. If the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $100,000 or more, or if the person fraudulently uses the personal identification information of 30 or more individuals without their consent, notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a

mandatory minimum sentence of 10 years' imprisonment.

(3) Neither paragraph (2)(b) nor paragraph (2)(c) prevents a court from imposing a greater sentence of incarceration as authorized by law. If the minimum mandatory terms of imprisonment imposed under paragraph (2)(b) or paragraph (2)(c) exceed the maximum sentences authorized under s. 775.082, s. 775.084, or the Criminal Punishment Code under chapter 921, the mandatory minimum sentence must be imposed. If the mandatory minimum terms of imprisonment under paragraph (2)(b) or paragraph (2)(c) are less than the sentence that could be imposed under s. 775.082, s. 775.084, or the Criminal Punishment Code under chapter 921, the sentence imposed by the court must include the mandatory minimum term of imprisonment as required by paragraph (2)(b) or paragraph (2)(c).

(4) Any person who willfully and without authorization possesses, uses, or attempts to use personal identification information concerning an individual without first obtaining that individual's consent, and who does so for the purpose of harassing that individual, commits the offense of harassment by use of personal identification information, which is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(5) If an offense prohibited under this section was facilitated or furthered by the use of a public record, as defined in s. 119.011, the offense is reclassified to the next higher degree as follows:

(a) A misdemeanor of the first degree is reclassified as a felony of the third degree.

(b) A felony of the third degree is reclassified as a felony of the second degree.

(c) A felony of the second degree is reclassified as a felony of the first degree.

For purposes of sentencing under chapter 921 and incentive gain-time eligibility under chapter 944, a felony offense that is reclassified under this subsection is ranked one level above the ranking under s. 921.0022 of the felony offense committed, and a misdemeanor offense that is reclassified under this subsection is ranked in level 2 of the offense severity ranking chart in s. 921.0022.

(6) Any person who willfully and without authorization fraudulently uses personal identification information concerning an individual who is less than 18 years of age without first obtaining the consent of that individual or of his or her legal guardian commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(7) Any person who is in the relationship of parent or legal guardian, or who otherwise exercises custodial authority over an individual who is less than 18 years of age, who willfully and fraudulently uses personal identification information of that individual commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(8)

(a) Any person who willfully and fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning a deceased individual commits the offense of fraudulent use or possession with intent to use personal identification information of a deceased individual, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) Any person who willfully and fraudulently uses personal identification information concerning a deceased individual commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $5,000 or more, or if the person fraudulently uses the personal identification information of 10 or more but fewer than 20 deceased individuals. Notwithstanding any other provision of law, the court shall sentence any person convicted of committing the offense described in this paragraph to a mandatory minimum sentence of 3 years' imprisonment.

(c) Any person who willfully and fraudulently uses personal identification information concerning a deceased individual commits the offense of aggravated fraudulent use of the personal identification information of multiple deceased individuals, a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $50,000 or more, or if the person fraudulently uses the personal identification information of 20 or more but fewer than 30 deceased individuals. Notwithstanding any other provision of law, the court shall sentence any person convicted of the offense described in this paragraph to a minimum mandatory sentence of 5 years' imprisonment. If the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $100,000 or more, or if the person fraudulently uses the personal identification information of 30 or more deceased individuals, notwithstanding any other provision of law, the court shall sentence any person convicted of an offense described in this paragraph to a mandatory minimum sentence of 10 years' imprisonment.

(9) Any person who willfully and fraudulently creates or uses, or possesses with intent to fraudulently use, counterfeit or fictitious personal identification information concerning a fictitious individual, or concerning a real individual without first obtaining that real individual's consent, with intent to use such counterfeit or fictitious personal identification information for the purpose of committing or facilitating the commission of a fraud on another person, commits the offense of fraudulent creation or use, or possession with intent to fraudulently use, counterfeit or fictitious personal identification information, a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(10) Any person who commits an offense described in this section and for the purpose of obtaining or using personal identification information misrepresents himself or herself to be a law enforcement officer; an employee or representative of a bank, credit card company, credit counseling company, or credit reporting agency; or any person who wrongfully represents that he

or she is seeking to assist the victim with a problem with the victim's credit history shall have the offense reclassified as follows:

(a) In the case of a misdemeanor, the offense is reclassified as a felony of the third degree.

(b) In the case of a felony of the third degree, the offense is reclassified as a felony of the second degree.

(c) In the case of a felony of the second degree, the offense is reclassified as a felony of the first degree.

(d) In the case of a felony of the first degree or a felony of the first degree punishable by a term of imprisonment not exceeding life, the offense is reclassified as a life felony.

For purposes of sentencing under chapter 921, a felony offense that is reclassified under this subsection is ranked one level above the ranking under s. 921.0022 or s. 921.0023 of the felony offense committed, and a misdemeanor offense that is reclassified under this subsection is ranked in level 2 of the offense severity ranking chart.

(11) The prosecutor may move the sentencing court to reduce or suspend the sentence of any person who is convicted of a violation of this section and who provides substantial assistance in the identification, arrest, or conviction of any of that person's accomplices, accessories, coconspirators, or principals or of any other person engaged in fraudulent possession or use of personal identification information. The arresting agency shall be given an opportunity to be heard in aggravation or mitigation in reference to any such motion. Upon good cause shown, the motion may be filed and heard in camera. The judge hearing the motion may reduce or suspend the sentence if the judge finds that the defendant rendered such substantial assistance.

(12) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of this state or any of its political subdivisions, of any other state or its political subdivisions, or of the Federal Government or its political subdivisions.

(13)

(a) In sentencing a defendant convicted of an offense under this section, the court may order that the defendant make restitution under s. 775.089 to any victim of the offense. In addition to the victim's out-of-pocket costs, restitution may include payment of any other costs, including attorney's fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of the actions of the defendant.

(b) The sentencing court may issue such orders as are necessary to correct any public record that contains false information given in violation of this section.

(14) Prosecutions for violations of this section may be brought on behalf of the state by any state attorney or by the statewide prosecutor.

(15) The Legislature finds that, in the absence of evidence to the contrary, the location where a victim gives or fails to give consent to the use of personal identification information is the county where the victim generally resides.

(16) Notwithstanding any other provision of law, venue for the prosecution and trial of violations of this section may be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides.

(17) A prosecution of an offense prohibited under subsection (2), subsection (6), or subsection (7) must be commenced within 3 years after the offense occurred. However, a prosecution may be commenced within 1 year after discovery of the offense by an aggrieved party, or by a person who has a legal duty to represent the aggrieved party and who is not a party to the offense, if such prosecution is commenced within 5 years after the violation occurred.

D. The Computer Fraud And Abuse Act, 18 U.S.C. § 1030 (2010)

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this

section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction

for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for—

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

(d)

(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered

into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;

(6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually,

during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section[.]

E. Acts of Terrorism Transcending National Boundaries 18 U.S.C. § 2332b (2010)

(a) **Prohibited Acts.—**
(1) **Offenses.—** Whoever, involving conduct transcending national boundaries and in a circumstance described in subsection (b)—
(A) kills, kidnaps, maims, commits an assault resulting in serious bodily injury, or assaults with a dangerous weapon any person within the United States; or
(B) creates a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the United States or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the United States;

in violation of the laws of any State, or the United States, shall be punished as prescribed in subsection (c).
(2) **Treatment of threats, attempts and conspiracies.—** Whoever threatens to commit an offense under paragraph (1), or attempts or conspires to do so, shall be punished under subsection (c).
(b) **Jurisdictional Bases.—**
(1) **Circumstances.—** The circumstances referred to in subsection (a) are—
(A) the mail or any facility of interstate or foreign commerce is used in furtherance of the offense;
(B) the offense obstructs, delays, or affects interstate or foreign commerce, or would have so obstructed, delayed, or affected interstate or foreign commerce if the offense had been consummated;
(C) the victim, or intended victim, is the United States Government, a member of the uniformed services, or any official, officer, employee, or agent of the legislative, executive, or judicial branches, or of any department or agency, of the United States;
(D) the structure, conveyance, or other real or personal property is, in whole or in part, owned, possessed, or leased to the United States, or any department or agency of the United States;
(E) the offense is committed in the territorial sea (including the airspace above and the seabed and subsoil below, and artificial islands and fixed structures erected thereon) of the United States; or
(F) the offense is committed within the special maritime and territorial jurisdiction of the United States.
(2) **Co-conspirators and accessories after the fact.—** Jurisdiction shall exist over all principals and co-conspirators of an offense under this section, and accessories after the fact to any offense under this section, if at least one of the circumstances described in subparagraphs (A) through (F) of paragraph (1) is applicable to at least one offender.
(c) **Penalties.—**
(1) **Penalties.—** Whoever violates this section shall be punished—
(A) for a killing, or if death results to any person from any other conduct prohibited by this section, by death, or by imprisonment for any term of years or for life;
(B) for kidnapping, by imprisonment for any term of years or for life;
(C) for maiming, by imprisonment for not more than 35 years;
(D) for assault with a dangerous weapon or assault resulting in serious bodily injury, by imprisonment for not more than 30 years;
(E) for destroying or damaging any structure, conveyance, or other real or personal property, by imprisonment for not more than 25 years;
(F) for attempting or conspiring to commit an offense, for any term of years up to the maximum punishment that would have applied had the offense been completed; and
(G) for threatening to commit an offense under this section, by imprisonment for not more than 10 years.
(2) **Consecutive sentence.—** Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section; nor shall the term of

imprisonment imposed under this section run concurrently with any other term of imprisonment.
(d) **Proof Requirements.—** The following shall apply to prosecutions under this section:
(1) **Knowledge.—** The prosecution is not required to prove knowledge by any defendant of a jurisdictional base alleged in the indictment.
(2) **State law.—** In a prosecution under this section that is based upon the adoption of State law, only the elements of the offense under State law, and not any provisions pertaining to criminal procedure or evidence, are adopted.
(e) **Extraterritorial Jurisdiction.—** There is extraterritorial Federal jurisdiction—
(1) over any offense under subsection (a), including any threat, attempt, or conspiracy to commit such offense; and
(2) over conduct which, under section 3, renders any person an accessory after the fact to an offense under subsection (a).
(f) **Investigative Authority.—** In addition to any other investigative authority with respect to violations of this title, the Attorney General shall have primary investigative responsibility for all Federal crimes of terrorism, and any violation of section 351 (e), 844 (e), 844 (f)(1), 956 (b), 1361, 1366 (b), 1366 (c), 1751 (e), 2152, or 2156 of this title, and the Secretary of the Treasury shall assist the Attorney General at the request of the Attorney General. Nothing in this section shall be construed to interfere with the authority of the United States Secret Service under section 3056.
(g) **Definitions.—** As used in this section—
(1) the term "conduct transcending national boundaries" means conduct occurring outside of the United States in addition to the conduct occurring in the United States;
(2) the term "facility of interstate or foreign commerce" has the meaning given that term in section 1958 (b)(2);
(3) the term "serious bodily injury" has the meaning given that term in section 1365 (g)(3);
(4) the term "territorial sea of the United States" means all waters extending seaward to 12 nautical miles from the baselines of the United States, determined in accordance with international law; and
(5) the term "Federal crime of terrorism" means an offense that—
(A) is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct; and
(B) is a violation of—
(i) section 32 (relating to destruction of aircraft or aircraft facilities), 37 (relating to violence at international airports), 81 (relating to arson within special maritime and territorial jurisdiction), 175 or 175b (relating to biological weapons), 175c (relating to variola virus), 229 (relating to chemical weapons), subsection (a), (b), (c), or (d) of section 351 (relating to congressional, cabinet, and Supreme Court assassination and kidnaping), 831 (relating to nuclear materials), 832 (relating to participation in nuclear and weapons of mass destruction threats to the United States) 842(m) or (n) (relating to plastic explosives), 844(f)(2) or (3) (relating to arson and bombing of Government property risking or causing death), 844(i) (relating to arson and bombing of property used in interstate commerce), 930(c) (relating to killing or attempted killing during an attack on a Federal facility with a dangerous weapon), 956(a)(1) (relating to

conspiracy to murder, kidnap, or maim persons abroad), 1030(a)(1) (relating to protection of computers), 1030(a)(5)(A) resulting in damage as defined in 1030(c)(4)(A)(i)(II) through (VI) (relating to protection of computers), 1114 (relating to killing or attempted killing of officers and employees of the United States), 1116 (relating to murder or manslaughter of foreign officials, official guests, or internationally protected persons), 1203 (relating to hostage taking), 1361 (relating to government property or contracts), 1362 (relating to destruction of communication lines, stations, or systems), 1363 (relating to injury to buildings or property within special maritime and territorial jurisdiction of the United States), 1366(a) (relating to destruction of an energy facility), 1751(a), (b), (c), or (d) (relating to Presidential and Presidential staff assassination and kidnaping), 1992 (relating to terrorist attacks and other acts of violence against railroad carriers and against mass transportation systems on land, on water, or through the air), 2155 (relating to destruction of national defense materials, premises, or utilities), 2156 (relating to national defense material, premises, or utilities), 2280 (relating to violence against maritime navigation), 2281 (relating to violence against maritime fixed platforms), 2332 (relating to certain homicides and other violence against United States nationals occurring outside of the United States), 2332a (relating to use of weapons of mass destruction), 2332b (relating to acts of terrorism transcending national boundaries), 2332f (relating to bombing of public places and facilities), 2332g (relating to missile systems designed to destroy aircraft), 2332h (relating to radiological dispersal devices), 2339 (relating to harboring terrorists), 2339A (relating to providing material support to terrorists), 2339B (relating to providing material support to terrorist organizations), 2339C (relating to financing of terrorism), 2339D (relating to military-type training from a foreign terrorist organization), or 2340A (relating to torture) of this title;
(ii) sections 92 (relating to prohibitions governing atomic weapons) or 236 (relating to sabotage of nuclear facilities or fuel) of the Atomic Energy Act of 1954 (42 U.S.C. 2122 or 2284);
(iii) section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with a dangerous weapon), section 46505 (b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life by means of weapons, on aircraft), section 46506 if homicide or attempted homicide is involved (relating to application of certain criminal laws to acts on aircraft), or section 60123 (b) (relating to destruction of interstate gas or hazardous liquid pipeline facility) of title 49; or
(iv) section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).

