

CSE 4201

Ethical Issues and Professional Practice in Computing

University of Guyana
Lecturer: Muriana McPherson
Semester 2: 2018/2019

Computer Security Issues as Distinct from Computer Crime

- ▶ Computer security concerns often overlap with issues analyzed under the topic of computer crime.
- ▶ Virtually all (known) violations of security involving computers and cybertechnology are also criminal in nature.
- ▶ But not every instance of crime in cyberspace necessarily involves a breach or violation of computer/cyber security.
- ▶ Consider, for example, that someone can use a computer or an electronic device to:
 - make unauthorized copies of software programs;
 - stalk a victim in cyberspace; bully someone online;
 - elicit sex with young children; distribute child pornography;
- Note: none of these (criminal) acts are a direct result of insecure computer systems.

Security as Related to Privacy

- ▶ Cyber-related issues involving privacy and security often overlap.
- ▶ But some important distinctions can also be drawn between the two notions.
- For example, privacy-related concerns often arise because users are concerned about losing control over ways in which personal information about them can be accessed by organizations (especially by businesses and government agencies), who claim to have some *legitimate* need for that personal information in order to make important decisions.
- This is not the case with security-related concerns.

Security as Related to Privacy (continued)

- ▶ Cyber-related security concerns (unlike those of privacy) typically arise because of either:
 - a) fears that many individuals and organizations have that their data could be accessed by those who have no legitimate need for, or right to, such information;
 - b) worries that personal data or proprietary information, or both, could be retrieved and possibly altered by individuals and organizations who are not authorized to access that data.

Security as Related to Privacy (continued)

- ▶ Privacy and security concerns can also be viewed as two sides of a single coin, where each side of the coin also complements and completes the other.
- ▶ Because securing personal information stored in computer databases is an important element in helping individuals to achieve and maintain their privacy, the objectives of privacy would seem compatible with (and complementary to) security.
- ▶ When cyberethics issues are examined from the perspective of security in cyberspace, the goals of protecting anonymity and individual autonomy seem less important than when cyberethics concerns are analyzed from the vantage-point of personal privacy.

Computer Security

- ▶ Neumann (2004) notes that computer security can be a “double-edged sword,” because it can be used both to:
 - a) protect privacy,
 - b) undermine freedom of access for users.

Three Aspects of Cybersecurity: Data, System, and Network Security

- ▶ Security issues involving cybertechnology span concerns having to do with three distinct kinds of (computer-related) vulnerabilities, which include:
 - I. unauthorized access to *data*, which either is resident in or exchanged between computer systems (i.e., *data security*);
 - II. attacks on *system* resources (such as computer hardware, operating system software, and application software) by malicious computer programs (i.e., *system security*);
 - III. attacks on computer *networks*, including the infrastructure of privately owned networks and the Internet itself (i.e., *network security*).

Data Security: Confidentiality, Integrity, and Availability of Information

- ▶ *Data security* is concerned with vulnerabilities pertaining to unauthorized access to data that can either:
 - a) reside in one or more computer storage devices,
 - b) be exchanged between two or more computer systems.
- ▶ Data-security issues affect the confidentiality, integrity, and availability of that information.

System Security

- ▶ *System security* is concerned with vulnerabilities to system resources such as computer hardware, operating system software, and application software.
- ▶ It is also concerned with various kinds of viruses, worms, and related “malicious programs” that can disrupt and sometimes destroy computer systems.

Network Security

- ▶ *Network security* is concerned with securing a wide range of computer networks - from privately owned computer networks (such as LANs and WANs) to the Internet itself - against various kinds of attacks.
- ▶ The Internet's infrastructure, which includes the set of protocols that makes communication across individual (or privately owned) computer networks possible, has been the victim of several attacks.
- ▶ Attacks on computer networks have ranged from programs launched by individuals and organizations whose intentions were malicious to those (individuals and organizations) claiming that their intentions were benign.

“Cloud Computing” and Security

...a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services). (NIST)

► Four Deployment Models

- Private Cloud,
- Community Cloud,
- Public Cloud,
- Hybrid Cloud.

► Three *service* (or *delivery*) models:

- Software as a Service (or SaaS),
- Platform as a Service (PaaS),
- Infrastructure as a Service (IaaS).

Securing User Data Residing in the Cloud

- ▶ One concern has to do with how users can control their data stored in the cloud - e.g., at present, users have very little “control over or direct knowledge about how their information is transmitted, processed, or stored”
- ▶ A second concern involves the integrity of the data - for example, if the host company goes out of business, what happens to the users’ data?
- ▶ A third kind of concern affects questions about access to the data - i.e., can the host deny a user access to his/her own data?
- ▶ A fourth concern has to do with who actually “owns” the data that is stored in the cloud

Assessing *Risk* in the Context of Cloud Computing

- ▶ Bruce Schneier (2004), who argues that security is an “ongoing process,” believes that a key element in that process involves an understanding of the concept of risk.
- ▶ Pieters and van Cleeff point out that because the information security landscape has become increasingly “de-perimeterized,” IT systems now “span the boundaries of multiple parties” and they “cross the security perimeters.”
- ▶ They also note that de-perimeterization-related concerns lead to “uncertain risk” for IT security, because of the lack of clear boundaries defining the security landscape with no secure “digital fence” or perimeter safeguarding the users' data.
- ▶ So both ordinary users and businesses may be required to assume some level of *uncertain risk* with regard to their data and system resources that reside in the cloud.

Ethical Aspects of Cybersecurity

- ▶ Ethical issues affecting individual autonomy, privacy, and expectations of anonymity arise because of cybersecurity.
- ▶ To realize autonomy, as well as privacy and anonymity, users need to have some control over how personal information about them is gathered and used.
- ▶ An ethical analysis of cybersecurity issues needs to consider whether an appropriate balance can be found in preserving both:
 - a) adequately secure computer systems;
 - b) autonomy and privacy for computer users.

Hacking and the “Hacker Ethic”

- ▶ Individuals and groups that launch malicious programs of various kinds are commonly described in the media as *hackers*.
- ▶ According to Simpson (2006), a hacker is anyone who “accesses a computer system or network without authorization from the owner.”
- ▶ “Early computer hackers” have been described as individuals who aimed at accessing computer systems to see how they worked, and not to cause any harm to those systems.
- ▶ Were these kinds of hackers also behaving unethically?
- ▶ These individuals are sometimes described as behaving in accordance with a certain “code of ethics.”

Hacking and the “Hacker Ethic” (Continued)

- ▶ Steven Levy (2001) describes the “Hacker Ethic” as comprising the following beliefs:
 - i. Access to computers should be unlimited and total.
 - ii. All information should be free.
 - iii. Mistrust Authority - Promote Decentralization.
 - iv. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
 - v. You can create art and beauty on a computer.
 - vi. Computers can change life for the better.

Hacking Activities

- ▶ Some hacking activities can be viewed as examples of three of the principles included in Levy's "Hacker Ethic":
 - 1) information should be (totally) free;
 - 2) hackers provide society with a useful and important service;
 - 3) activities in cyberspace are virtual in nature; so they do not cause real harm to people in the real (physical) world.

“Information Wants to Be Free”

- ▶ Should all information be totally free?
- ▶ The view that information should be free is regarded by some critics (for example, Spafford 2004) as naïve, idealistic, or romantic.
- ▶ Spafford notes that if information were free:
 - privacy would not be possible because we would not be able to control how information about us was collected and used.
 - it would not be possible to ensure integrity and accuracy of that information.

Do Hackers Really Provide an Important Service?

- ▶ Spafford also provides counterexamples to this version of the “hacker argument.”
- ▶ He asks whether we would permit someone to start a fire in a crowded shopping mall in order to expose the fact that the mall's sprinkler system was not adequate.
- ▶ Alternatively, would you be willing to thank a burglar who successfully broke into your house?
- For example, would you thank that burglar for showing that your home security system was inadequate?

Does Hacking Causes Only Virtual Harm, Not Real Harm?

- ▶ Some argue that break-ins and vandalism in cyberspace cause no “real harm” to persons because they are activities that occur only in the *virtual realm*.
- ▶ This argument commits a logical fallacy by confusing the connection between the real and the virtual regarding harm by reasoning in the following way:
 - *The virtual world is not the real (physical) world; so any harms that occur in the virtual world are not real harms. (James Moor calls this the *Virtuality Fallacy*.)*

Can Computer Break-ins Ever Be Ethically Justified?

- ▶ Spafford suggests that in certain extreme cases, breaking into a computer could be the "right thing to do." eg., breaking into a computer to get medical records to save one's life.
- ▶ Spafford seems to use a deontological (or non-consequentialist) argument to justify the break-in the case of the medical emergency. Eg., Spafford believes that morality is determined by *actions not results*.
- ▶ He argues that we cannot evaluate morality based on consequences or results because we would not "know the full scope of those results," which are based on the "sum total of all future effect."
- ▶ Spafford's argument tends to be based on a version of *act deontology*.

Malicious Hackers and “Hacking Tools” on the Internet

- ▶ Simpson (2006) notes that many malicious hackers do not possess outstanding technical skills.
- However, they know how to locate sophisticated “hacking tools” that can be downloaded from the Internet for free.
- ▶ Many of these individuals also know how to take advantage of “holes” in computer systems.
- ▶ Some programmers refer to these “hackers” as “script kiddies” or “packet monkeys,” since they copy code from knowledgeable programmers as opposed to creating the code themselves.

Counter Hacking or “Hacking Back” (Active Defense Hacking)

- ▶ Can *counter hacking* or “hacking back” (at hackers) be justified?
- ▶ Counter hacking has been done both by individuals and corporations.
- ▶ Counter-hacking attacks are typically directed against those suspected of originating the hacker attacks.
- ▶ Counter hacking can be either *preemptive* or *reactive*.
- ▶ Both forms are controversial, but preemptive counter hacking is more difficult to defend.
- ▶ Is counter hacking an act of *self-defense*, or is it simply another case of “two wrongs making a right”?

Counter Hacking (Continued)

- ▶ Because counter hacking can cause harm to innocent individuals, some question whether it can be defended on moral grounds.
- ▶ Himma (2008) notes that in cases of hacking back against *denial of service* (DoS) attacks, many innocent persons are adversely affected because the attacks are routed through their computer systems.
- ▶ Hackers can use the computers of innocent persons as “host computers” to initiate their attacks.
- This technique is called “IP spoofing.”
- ▶ Victims assume that the attacks originated from the host computer, rather than from the actual computer that initiated the attack.
- ▶ So when victims hack back, they can unintentionally cause the intermediate computer to be assaulted by bogus requests for service.

Certified Ethical Hackers

- ▶ Certified Ethical Hackers (CEH) are trained and *certified* in counter hacking.
- ▶ Not only are they trained in the use of defensive measures, but some are also authorized to engage in security-related activities that involve *preemptive* strikes as well.
- ▶ The goal of the ethical hacker is to help the organization take *preemptive measures* against malicious attacks by attacking the system himself; all the while staying within legal limits.
- ▶ **Should it be legal to for Certified Ethical Hackers to engage in preemptive hacking attacks?**
- ▶ Some who defend preemptive acts of counter hacking believe that they can be justified on utilitarian, or consequentilaist, grounds.
- For example, they argue that less overall harm will likely result if preemptive strikes are allowed.
- ▶ However, it would seem that many of the same difficulties that apply to utilitarian arguments would apply here as well.

Cyberterrorism

- ▶ Dorothy Denning (2004, 2007) defines *cyberterrorism* as the "convergence of cyberspace and terrorism."
- ▶ Cyberterrorism covers a range of politically motivated hacking operations intended to cause grave harm that can result in either loss of life or severe economic loss, or both.
- ▶ In some cases, it is difficult to separate acts of cyberterrorism from cybervandalism and cyberwarfare, and acts of ordinary hacking.

Cyberterrorism vs. Hacktivism

- ▶ *Denial-of-service* (DoS) attacks have been launched for the purpose of preventing users from accessing targeted commercial Web sites.
- ▶ These attacks have also resulted in severe economic loss for major corporations.
- ▶ Should these DoS-related attacks necessarily be classified as instances of cyberterrorism?
- ▶ Or, can some of these attacks be better understood as another form of malicious hacking - i.e., those perpetrated by persons or groups with a particular political agenda or ideology?
- ▶ They also question whether the behavior of these persons and groups suggests a new form of civil disobedience, which they describe as *hacktivism*.

Can Hacktivism be Justified?

- ▶ Himma (2007) describes the line of reasoning that hacktivists and their supporters tend to use to justify their activities as forms of political activism and “electronic civil disobedience” (or ECD):
 - **PREMISE 1.** Because civil disobedience is justifiable as a protest against injustice, it is permissible to commit digital intrusions as a means of protesting injustice.
 - **PREMISE 2.** In so far as it is permissible to stage a sit-in in a commercial or governmental building to protest, say laws that violate human rights, it is permissible to intrude on commercial or government networks to protest such laws.
 - **CONCLUSION.** Digital intrusions that would otherwise be morally objectionable are morally permissible if they are politically motivated acts of electronic civil disobedience, or hacktivism.

Hactivism as a form of Electronic Civil Disobedience (ECD)

- ▶ With regard to ECD, Manion and Goodrum (2004) claim that for an act to qualify as “civilly disobedient,” it must satisfy the following conditions:
 - No damage done to persons or property;
 - Nonviolent;
 - Not for personal profit;
 - Ethical motivation - the strong conviction that a law is unjust, or unfair, to the extreme detriment of the common good;
 - Willingness to accept personal responsibility for the outcome of actions.

Hacktivism as a form of ECD (Continued)

- ▶ Denning (2008) argues that Manion and Goodrum's analysis of hacktivism suggests that some acts of Web defacement may also be morally justified as ECD, in so far as they are "ethically motivated."
- ▶ But Denning points out that defacing a Web site seems to be incompatible with Manion and Goodrum's first condition for ECD - i.e., "no damage."
- ▶ For example, she notes that defacements can "cause information property damage that is analogous to physical property damage" and both can "require resources to repair."

Activism, Hacktivism, and Cyberterrorism

- ▶ *Activism* includes the normal, non-disruptive use of the Internet to support a cause.
- For example, an activist could use the Internet to discuss issues, form coalitions, and plan and coordinate activities.
- ▶ Activists could engage in a range of activities from browsing the Web to sending e-mail, posting material to a Web site, constructing a Web site dedicated to their political cause or causes, and so forth.

Activism, Hacktivism, and Cyberterrorism

- ▶ Hacktivism is the *convergence of activism and computer hacking*.
- ▶ It uses hacking techniques against a target Internet site with intent to disrupt normal operations, but without intending to cause serious damage.
- ▶ These disruptions could be caused by "e-mail bombs" and "low grade" viruses that cause only minimal disruption, and would not result in severe economic damage or loss of life.

Activism, Hacktivism, and Cyberterrorism (continued)

- ▶ Cyberterrorism consists of operations that are intended to cause great harm such as loss of life or severe economic damage, or both.
- For example, a cyberterrorist might attempt to bring down the U.S. stock market or take control of a transportation unit in order to cause trains to crash.
- ▶ Denning believes that conceptual distinctions can be used to differentiate various activities included under the headings of activism, hacktivism, and cyberterrorism.

Cybertechnology and Terrorist Organizations

- ▶ Some members of al Qaeda and ISIS now possess very sophisticated computer devices, as well as the skills needed to use them effectively, despite the fact that many also operate in remote regions of the world.
- ▶ In the November 2015 terrorist attacks in France, ISIS terrorists used encryption technology to communicate with one another in ways that made it extremely difficult for European authorities to monitor and intercept those communications.
- ▶ When al Qaeda terrorists flew airplanes into the Twin Towers, on 9/11, they had to take their own lives in the act.
- ▶ But we can imagine that would happen if terrorists are someday able to gain control of onboard computer systems on airplanes and override the airplane's computerized controls.

Cybertechnology & Terrorism

- ▶ Denning (2007) noted that the evidence then suggested that terrorists groups and “jihadists” were interested in conducting cyberattacks, and that these terrorist groups had at least some capability to carry out such attacks.
 - For example, she noted that they were undergoing online training on how to develop the necessary skills.
- ▶ But Denning also pointed out that at that time, there was no evidence to suggest either that:
 - the threat of cyberattacks from these groups was imminent;
 - These groups had acquired the knowledge or the skills to conduct “highly damaging attacks against critical infrastructure.”

Information Warfare

- ▶ Denning (1999) defines *information warfare* (IW) as "operations that target or exploit information media in order to win some objective over an adversary."
 - For example, IW need not involve loss of life or severe economic loss, even if such results can occur.
- ▶ IW, unlike conventional or physical warfare, tends to be *more disruptive than destructive*.
- ▶ The instruments of war in IW typically strike at a nation's infrastructure.
- ▶ The kinds of "weapons" used typically consist of malware (including viruses and worms), as well as DoS attacks (described earlier).
- ▶ The disruption caused by malware and DoS attacks can be more damaging, in many respects, than physical damage caused to a nation by conventional weapons.

Information Warfare (continued)

- ▶ Moor (2004) notes that in the computer era, the concept of warfare has become “informationally enriched.”
- ▶ Moor also notes that while information has always played a vital role in warfare, now its importance is overwhelming, because the “battlefield is becoming increasingly computerized.”
- ▶ Moor and others note that in the past, warfare was conducted by physical means - e.g., human beings engaged in combat, using weapons such as guns, tanks, and aircraft.
- ▶ But during the first Gulf War, in the early 1990s, we saw for the first time the importance of information technology in contemporary warfare strategies.

The GhostNet Controversy

In 2009, The Information Warfare Monitor (IWM), a Canadian organization that monitors cyberespionage, discovered a network of at least 1,295 compromised computers in 103 countries. Approximately 30% of these were considered “high-value” targets, which (according to the IWM Report) included ministries of foreign affairs, embassies, international organizations, news media, and nongovernmental organizations (NGOs). The computer systems were compromised in ways that suggested China was responsible, but the IWM report refused to identify any one nation. The circumstantial evidence implicating China was tied to the fact that IWM’s investigation was launched in response to a request by the Dali Lama, the exiled leader of Tibet (and long-time enemy of the Chinese government), who reported that his computer network had been hacked. (The IWM report referred to the cyberespionage system as “GhostNet” because it resembled the ghOst RAT Trojan horse malware that was traced back to Hainan, China.) The IWM report concluded that regardless of which country or countries were responsible for the cyberespionage, the discovery of these activities should serve as a warning to policy makers that network security requires serious attention.

Information Warfare (Continued)

- ▶ The GhostNet controversy (described in Scenario 6-2, in connection with network security) also has implications for IW.
- ▶ A report issued by the *Information Warfare Monitor* (2009) included circumstantial evidence that linked various cyberattacks (associated with GhostNet) to China, but also suggested that other countries might be involved as well.

Information Warfare (continued)

- ▶ In 2009, the government of South Korea accused North Korea of running a cyberwarfare unit that attempted to hack into both U.S. and South Korean military networks to gather confidential information and to disrupt service.
- ▶ North Korea was also suspected of launching the DoS attacks that disrupted the Web sites of 27 American and South Korean government agencies as well as commercial Web sites such as the New York Stock Exchange, Nasdaq, and Yahoo's finance section (Shang-Hun and Markoff 2009).

The Stuxnet Worm and the “Olympic Games” Operation

In June 2012, The New York Times reported that the U.S. and Israeli governments had been cooperating on an initiative code-named Olympic Games. First developed during the George W. Bush administration, this initiative aimed at disrupting Iran’s uranium enrichment program and thus damaging that nation’s nuclear capability (Charette 2012). At the core of this joint operation was a computer worm known as Stuxnet, a “cyberweapon” that targeted “electronic program controllers” developed by Siemens Corporation (in Germany) for industrial control computers (ICCs) that were installed in Iran. This worm was allegedly responsible for (a) sending misleading data to computer monitors in Iran, and (b) causing several of that nation’s centrifuges—i.e., fast-spinning machines that enrich uranium—to spin out of control. The Stuxnet attack is estimated to have destroyed approximately 1,000 of Iran’s 6,000 centrifuges (Nakashima and Warrick 2012).

Information Warfare (continued)

- ▶ Does “Operation Olympic Games” qualify as an instance of IW (or “cyberwarfare”)?
- ▶ In so far as the Stuxnet worm sent misleading information to the Iranian government and its scientists, it complies with one aspect of IW.
- ▶ Also, because this worm was *disruptive* (regarding Iran’s nuclear program), as well as *destructive* (i.e., with respect to its effect on Iran’s centrifuges), it complies with another aspect of IW.
- ▶ Consider that the Stuxnet attacks were launched (allegedly, at least) by two nation states.
- ▶ So, Stuxnet complies with all three elements of IW

Information Warfare (continued)

- ▶ It is perhaps also worth noting that in the Olympic Games incident, there had been no formal declaration of war among the three nation states allegedly involved.
- ▶ The Stuxnet worm, discovered in 2010, is sometimes confused with the Flame virus (also known as “Flamer” and “Skywiper”).
- ▶ The Flame virus also has implications for IW.
- ▶ Ladner (2012) points out that the Flame virus, discovered in 2012, is “an espionage tool” that can “eavesdrop on data traffic, take screenshots and record audio and keystrokes.”

Potential Consequences for Nations that Engage in IW

- ▶ In light of the Stuxnet attacks, some might ask if the U.S. and Israeli governments are now also guilty of the same kind of questionable behavior attributed to China and North Korea.
- ▶ Should the U.S. government worry about the possible repercussions that its involvement in “Olympic Games” could have for its standing in the international community, as well as for its credibility involving any future complaints that it might make against other nations, especially China?
- ▶ Sanger (2012) suggests that the United States did not think through the international implications of its use of cyberwarfare in the Olympic Games operations (just as he believes that it also did not think through some of the major political and legal consequences of its policy regarding use of armed drones).

Information Warfare and Requirements for “Just War”

- ▶ Some question whether IW can meet the conditions required for “just” warfare (i.e., a “just war”).
- ▶ One condition that must be satisfied for a just war to be carried out is that a distinction be made between combatants and noncombatants.
- ▶ Many critics worry that in the context of IW, it may not be possible to make this distinction (and other kinds of important distinctions) affecting just-war requirements.
- ▶ So, some have concluded that IW can never be justified solely on moral grounds.

Criteria for Determining Computer Crimes

- ▶ When is a crime a *computer crime*?
- ▶ What *criteria* should be used for determining that?
 - Some have suggested that all crimes involving either the use or the presence of a computer should count as (examples of) computer crimes.
 - But are all of these crimes necessarily computer crimes (and are they issues for computer ethics)?
- ▶ Gotterbarn (1995) asks whether a murder committed with a surgeon's scalpel is an issue for medical ethics.
 - If not, then why is a crime involving a computer an issue for computer ethics, and why is it a computer crime?

Criteria for Determining Computer Crimes (Continued)

- ▶ Do we need a separate category of computer crime/cybercrime?
- ▶ Review three hypothetical scenarios each describing a crime involving a computer lab:
 - *Scenario a:* Sandra steals a computer device (e.g., a printer) from a computer lab;
 - *Scenario b:* Bill breaks into a computer lab and then snoops around;
 - *Scenario c:* Ed enters a computer lab that he is authorized to use and then places an explosive device, which is set to detonate a short time later, on a mainframe computer in the lab.

Defining Computer Crime

- ▶ Robert Moore (2011) suggests that a computer crime can include “any criminal activity involving a computer” (while a cybercrime would include “any criminal activity involving a computer and a network”).
- ▶ Under Moore’s definition, each of the criminal activities described in Scenarios a, b, and c would seem to fall under the category “computer crime.”
- ▶ Forester and Morrison (1994) define a computer crime as “a criminal act in which a computer is used as the *principal tool*.”
- ▶ This definition rules out the criminal acts committed in the three scenarios involving a computer lab as “computer crimes.”

Defining Computer Crime (Continued)

- ▶ Review the scenario in which “Sheila” uses a computer to file a fraudulent income-tax return.
- ▶ Arguably, a computer is the *principal tool* used by Sheila to carry out the criminal act.
- ▶ So, on Forester and Morrison’s definition, Sheila’s criminal act might count as *computer crime* .
- ▶ Girasa (2002) defines "cybercrime" as
a generic term covering a multiplicity of crimes found in penal code or in legislation having the "use of computer technology as its central component."
- ▶ But what, exactly, is meant by “central component”?
- ▶ Was a computer a central component in the scenario where Sheila filed the fraudulent income tax form?

Defining Computer Crime (Continued)

- ▶ Strickwerda (2013) defines a cybercrime as
any new or different human act that is carried out through the use of computers or computer networks and is prohibited by the enactment of...law.
- ▶ Initially, this definition might not seem to be much of an improvement over the earlier definitions that we examined.
- ▶ One virtue of Strikweda's definition is in her insight that a cybercrime is *a new or different human act* (carried out by computers).
- ▶ This insight echoes James Moor's point that computers make possible "new kinds of human actions" and thus generate "policy vacuums" (Moor 2007).

Towards a Coherent Definition of Cybercrime

- ▶ We define a (genuine) cybercrime as a crime in which *the criminal act can*:
 - 1) *be carried out only through the use of cybertechnology, and*
 - 2) *take place only in the cyber realm.*
- ▶ Unlike the earlier definitions we considered, this one rules out the income-tax scenario as a genuine cybercrime, in addition to ruling out the three scenarios in the computer lab.

Genuine Cybercrimes

- ▶ Using our definition of cybercrime, we can further categorize genuine cybercrimes as follows:
- ▶ Cyberpiracy—using cybertechnology in unauthorized ways to
 - ▶ reproduce copies of proprietary information, or
 - ▶ distribute proprietary information (in digital form) across a computer network.
- ▶ Cybertrespass—using cybertechnology to gain unauthorized access to
 - ▶ an individual's or an organization's computer system, or
 - ▶ a password-protected Web site.
- ▶ Cybervandalism—using cybertechnology to unleash one or more programs that
 - ▶ disrupt the transmission of electronic information across one or more computer networks, including the Internet, or
 - ▶ destroy data resident in a computer or damage a computer system's resources, or both.

Examples of the Three Categories of (Genuine) Cybercrimes

- ▶ Consider three actual incidents:
 - 1) distributing copyrighted MP3 files (and other proprietary digital content) on illegal file-sharing sites such as The Pirate Bay;
 - 2) unleashing the Heartbleed Virus (2014);
 - 3) launching the Internet-wide denial-of-service attacks on commercial Web sites (2012).
- ▶ We can use our model of cybercrime to see where each incident would fall.

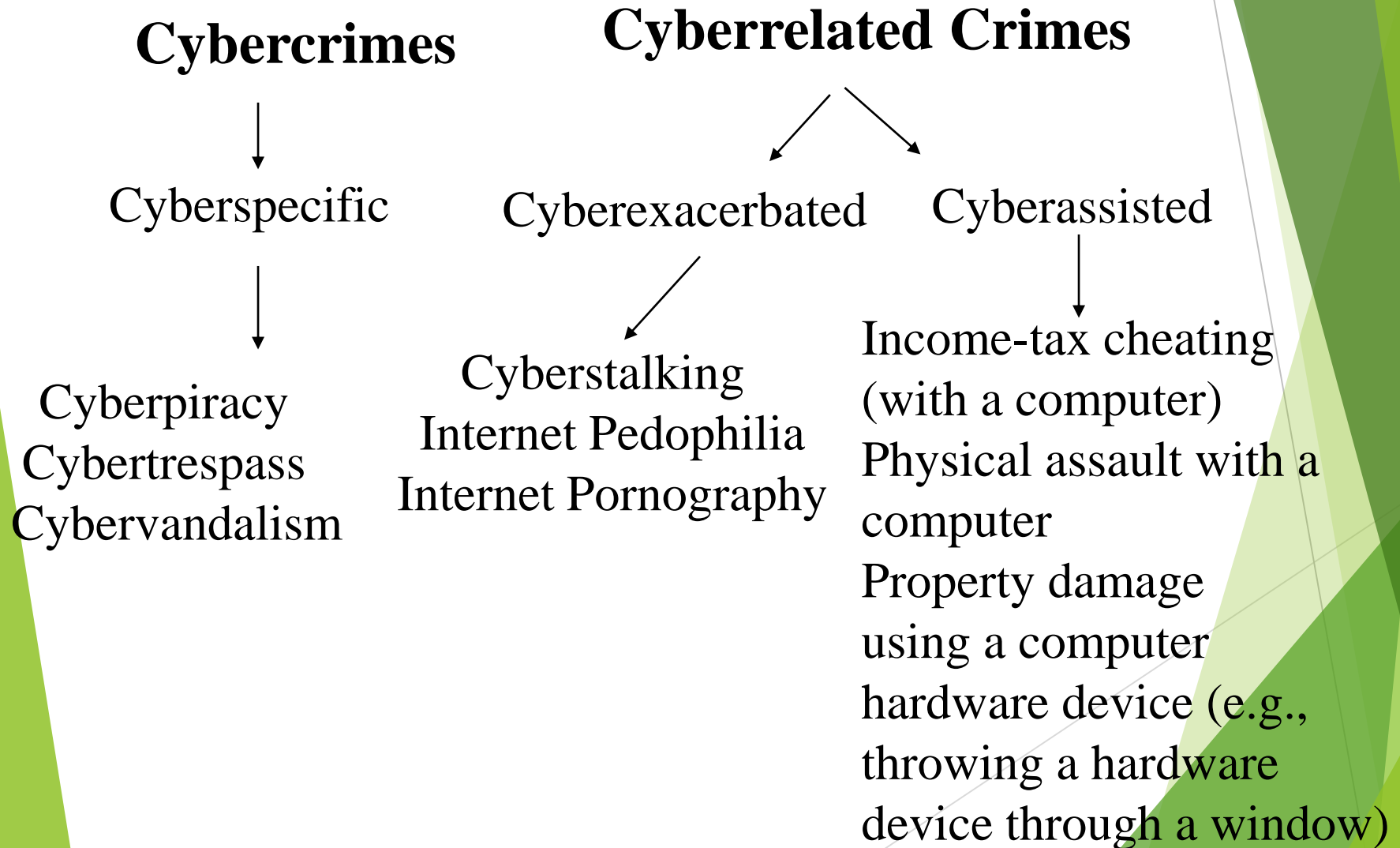
Distinguishing Cybercrimes from Cyber-related Crimes

- ▶ Many crimes that involve the use of cybertechnology are not *genuine* cybercrimes.
 - For example, crimes involving pedophilia, stalking, and pornography can be carried with or without the use of cybertechnology.
 - Nothing about these kinds of crimes is unique to, or requires the use of, cybertechnology.
 - These crimes are better understood as examples of *cyber-related* crimes.
- ▶ Cyber-*related* crimes can be further divided into two sub-categories:
 - i. *cyberexacerbated* crimes;
 - ii. *cyberassisted* crimes.

Cyber-exacerbated vs. Cyber-assisted crimes

- ▶ We can also further distinguish between a crime in which cybertechnology is used to:
 - a) (a) file a fraudulent income-tax return,
 - b) (b) stalk people, distribute pornography, solicit minors for sex.
- ▶ In (a), a computer *assists* in a way that is trivial and possibly irrelevant.
- ▶ In (b), cybertechnology has played a much more significant (i.e., an *exacerbating*) role.

Figure 7-1: Cybercrimes and Cyber-related Crimes



Identity Theft: A Cyber-related Crime

- ▶ Lininger and Vines (2005) define identity theft as a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate some else.
- ▶ They go on to note that the information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.
- ▶ Identity-theft crimes can also include the taking of another person's identity through the fraudulent acquisition of personal information in credit card numbers.
- ▶ Wall (2007) notes that identity theft is often mistakenly used to describe crimes involving credit card theft.

Identity Theft (Continued)

- ▶ Identity theft, like other cyber-related crimes, does not require cybertechnology.
- ▶ Identity thieves have been very successful in scams involving cybertechnology in general (e.g. in recording credit card “swipes”), independent of the Internet
- ▶ Many kinds of identity-theft scams have been carried out on the Internet.
- ▶ One common example is a scheme involving email that appears to be from a reputable business.
- For example, you may receive e-mail that looks like it was sent by eBay, Amazon, or PayPal.
- ▶ The emails often look legitimate because they include the official logos of the companies they claim to be.
- ▶ Some messages inform you that your account is about to expire and that you need to update it by verifying your credit card number.

National and International Efforts to Fight Cybercrime

- ▶ Problems of jurisdiction arise at both the national and international levels.
- ▶ Jurisdiction is based on the concept of boundaries, and laws are based on "territorial sovereignty" (Girasa, 2002).
- ▶ Cyberspace has no physical boundaries.

The Problem of Jurisdiction in Cyberspace

- ▶ Laws are typically limited in jurisdiction to nations where they are enacted. Some laws involving cybercrime are intended to have international reach, but issues involving legal jurisdiction have often impeded their prosecution in many instances.
- ▶ Traditionally, crimes are prosecuted in the legal jurisdictions in which they were committed. In certain cases, suspected criminals have been extradited from one legal jurisdiction to another to stand trial for an accused crime.
- ▶ Jurisdiction is based on the concept of boundaries, and laws are based on “territorial sovereignty.” Jurisdiction is the sovereign authority of a nation to make laws which are enforceable within its own territory
- ▶ Because cyberspace has no physical boundaries, it can be difficult to prosecute cybercrimes involving multiple nations. So, some have questioned whether the concept of legal jurisdiction makes any sense in cyberspace.

Jurisdictional Problems in Cyberspace (Scenario 7-5)

XYZ Corporation, a major computer company in the United States, has developed and released a new software product that has been distributed globally. However, this product has a serious defect that causes computer systems using it to crash under certain conditions. These system crashes, in turn, result in both severe disruption and damage to system resources. QTRON, a company headquartered in eastern Asia that purchased this product from XYZ, has experienced multiple system crashes since installing it, which has also resulted in a severe loss of revenue for that company. What legal recourse does/should QTRON have in its complaint against XYZ Corp., given that its complaint involves companies in two sovereign nations?

XYZ Corp. Scenario

- ▶ Suppose that XYZ develops and releases, globally, a software product that is defective.
- ▶ Further suppose that the software defect causes computer systems to crash under certain conditions, which can also result in severe disruption and damage to system resources.
- ▶ What recourse should consumers and organizations who purchase this product have in their complaint against XYZ Corp.?
- ▶ Suppose that several countries in which XYZ has sold its new product also have strict liability laws.
- ▶ Should XYZ Corp. be held legally liable in each country in which its defective product has been sold?
- ▶ Should that corporation then be forced to stand trial in each of these countries?

ENFORCING CYBERCRIME LAWS INVOLVING MULTIPLE NATIONS

The “I Love You letter” was a computer virus which was spread through an email attachment and which affected millions of personal computers and systems around the world in May 2000. The virus was created and disseminated by two computer programmers from the Philippines who were traced by the authorities and counterparts in that country. Since the Philippines did not have a law to punish crimes against the creation and dissemination of viruses at that time, the authorities in that country dropped all the charges against the offenders and they were not criminally prosecuted. This case took a relevant dimension when the United States Department of Justice got involved in the investigation and tried to cooperate in the prosecution and extradition of the offenders to the United States, however such efforts were meaningless precisely because of the principle and requirement of dual criminality, which requires that extradition may be allowed only when the legislation of both countries provides for a specific sanction and punishment, which was not the case in the Philippines.

- ▶ Even though it originated in the Philippines, its effect was global. Did an actual crime even occur? Furthermore, if no crime was committed by the Perpetrator in the Philippines, should he have been extradited to nations that do have cyber-related crime laws, and should he be required to stand trial in those nations?
- ▶ On the one hand, it might be argued that he should stand trial in any country that was affected by the virus he launched; after all, individuals and institutions in those countries were harmed by his act.
- ▶ On the other hand, would we want all cases of crimes or of controversial Internet practices that have a global reach prosecuted by multiple nations?
- ▶ Using the same rationale, would it follow that XYZ should be tried in each country where its defective product caused some damage?
- ▶ Consider that if XYZ were to be found guilty in these nations' courts, the economic results for that corporation could be catastrophic.

The Yahoo Case

- ▶ Yahoo has a website which auctions in France Nazi Memorabilia and Third Reich related goods. French law, however, prohibits the display in France of Nazi souvenirs for the purpose of sale.
- ▶ Moreover, the online sale of Nazi artifacts in France is considered as an offense on the memory of France which was severely wounded by the atrocities committed by the Nazis during World War II
- ▶ Yahoo argued that it is a company incorporated in the United States of America and the laws of France is not binding upon it. The French High Court ordered Yahoo to prohibit internet users in France from gaining access to the auction of Nazi-related objects. It was also ordered to remove these auctioned items in its server for being in violation of its laws

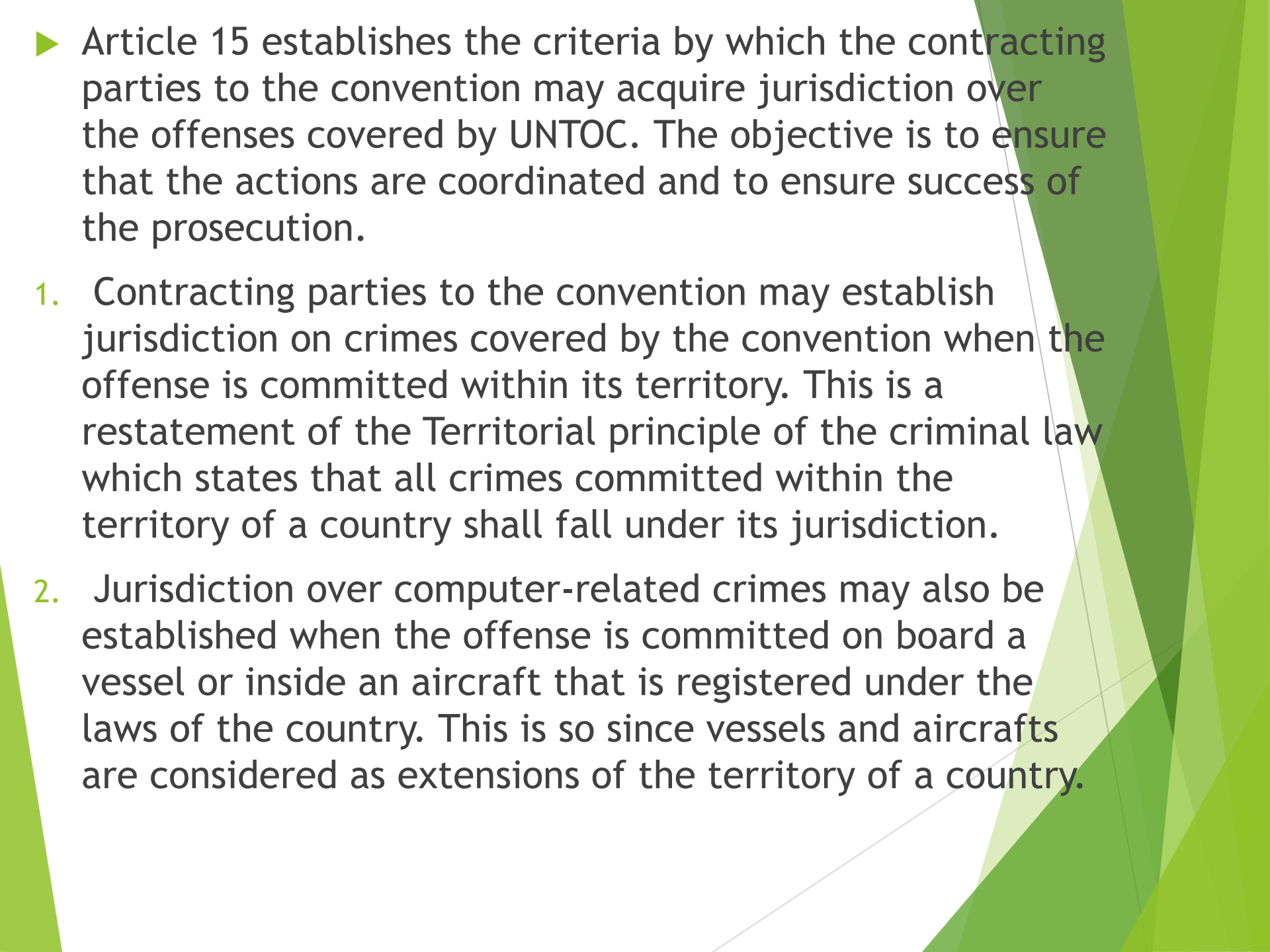
- ▶ The Yahoo case illustrates the possible complications that may arise when the laws of one country against cybercrime conflicts with the laws of another country. This also presents a thorny issue for a nation which wants to prosecute a cybercrime committed by perpetrator within the territory of another nation.
- ▶ What if the damage caused by the act of a cyber criminal reaches the territory behind borders?
- ▶ What if the committed act was not a crime in the country of action but considered a crime in the country that damage reaches its territory?
- ▶ If both countries want to file charges against the perpetrator which country shall be given priority?
- ▶ Which country has jurisdiction to file charges against the perpetrator of the crime?
- ▶ What if no state wants to file charges against the perpetrator of the crime?
- ▶ What should be the basis for claiming jurisdiction over the criminal act?
- ▶ Should it be the territory where the crime was committed or the nationality of the person committing the act or the country of residence of the perpetrator?

International Laws and Treaties to Combat Cybercrime

- ▶ the United Nations Convention on Transnational Organized Crime (*UNTOC*) - *adopted on November 15, 2000 by the UN General Assembly.*
- ▶ *Council of Europe (COE) cybercrime convention signed in 2001 by 30 countries. Currently 51 countries are signatories. Guyana is not currently a signatory*

United Nations Convention on Transnational Organized Crime (UNTOC).

- ▶ cybercrime is inextricably linked with organized criminal group. There is evidence that sophisticated criminal groups have taken advantage of internet technology for purpose of committing different crimes such as online pornography, hacking, money laundering, fraud and theft.
- ▶ cybercrime is transnational in nature. Section 3 states that an offense is transnational in nature if:
 - a. It is committed in more than one State;
 - b. It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;
 - c. It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State;
 - d. It is committed in one State but has substantial effects in another State

- 
- ▶ Article 15 establishes the criteria by which the contracting parties to the convention may acquire jurisdiction over the offenses covered by UNTOC. The objective is to ensure that the actions are coordinated and to ensure success of the prosecution.
 - 1. Contracting parties to the convention may establish jurisdiction on crimes covered by the convention when the offense is committed within its territory. This is a restatement of the Territorial principle of the criminal law which states that all crimes committed within the territory of a country shall fall under its jurisdiction.
 - 2. Jurisdiction over computer-related crimes may also be established when the offense is committed on board a vessel or inside an aircraft that is registered under the laws of the country. This is so since vessels and aircrafts are considered as extensions of the territory of a country.

3. Jurisdiction over computer-related crime may also be established when the victim or the perpetrator of the crime is a national of one of the contracting party to the UNTOC. Thus, even if the location of the crime is in a different country when the victim happens to be citizen of another country, the latter country may still acquire jurisdiction over the cybercrime.
4. The Jurisdiction may also be acquired by a contracting party to the UNTOC when a cybercrime is committed by a stateless person who habitually resides in the territory of the one of the signatories to the UNTOC.
5. Jurisdiction over cybercrime may also be acquired by a contracting party even when the crime is committed outside its territory if it is the intention of perpetrators of the crime to commit a serious crime within its territory, Thus, under the UNTOC, a contracting party acquires jurisdiction over a person who organizes, directs, aids, abets or facilitates the commission of cybercrime involving an organized crime even when it is outside its own territory provided that it can be established that there is an intention to commit the crime within the territory.

Council of Europe (COE)

- ▶ The COE Convention on Cybercrime considers four types of criminal activity in cyberspace:
 1. Offenses against the confidentiality, availability, and integrity of data and computer systems;
 2. Computer-related offenses (such as fraud);
 3. Content-related offenses (such as child pornography);
 4. Copyright-related offenses.

The main goal of the Cybercrime Convention is to provide for a common criminal policy by harmonizing national laws with the aim of protecting the society against cybercrime

The treaty requires signatories to

1. Define criminal offenses and sanctions under their own domestic laws for the four categories of computer-related
2. Establish domestic procedures for detecting, investigating and prosecuting computer crimes and collecting electronic evidence and to establish a rapid and effective system of international cooperation.
3. Follow defined procedures related to requests for mutual assistance, in the absence of enforced international agreements; and the necessity to maintain the confidentiality of information's request, the mutual assistance regarding the urgent precautionary procedures on stored computer data related to crime and the speed in detecting confidential stored data traffic and mutual assistance relating to each of: accessing stored computer data and crossing the limits, and accessing stored data in any geographic location, in a state, which is a party in an agreement; in addition to compiling the data traffic in a fast way and challenging data content.
4. to maintain a point of contact available on a twenty - four hour, seven days a week basis, for of investigations or proceedings concerning criminal offences related to cybercrimes to any of States Parties, or to collect evidence, or to provide technical advice, or to preserve the data.

Establishing a Security Policy

- ▶ Defines an organization's security requirements, as well as the controls and sanctions needed to meet those requirements.
- ▶ Delineates responsibilities and the behavior expected of members of the organization.
- ▶ Outlines what needs to be done but not how to do it.

When applying system security restrictions, there are some trade-offs between ease of use and increased security; however, when a decision is made to favor ease of use, security incidents sometimes increase.

- ▶ As security techniques continue to advance in sophistication, they become more transparent to end users.
- ▶ Employees, contractors, and part-time workers must be educated about the importance of security so that they will be motivated to understand and follow the security policies.