



**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

**UTeM**

# BITS 2523

## Cyberlaw & Security Policy

### Lecture 6

By

Mohd Fairuz Iskandar Othman, Phd

[mohdfairuz@utem.edu.my](mailto:mohdfairuz@utem.edu.my)

## Topics covered:

- Intro
- Sovereignty
- Jurisdiction
- Types of cybercrime: local & transnational
- Cyberspace as a criminal tool
- Issues of transnational cybercrime
- Prioritizing jurisdictional claims
- Summary

- The Internet's broad connectivity and the **difficulty of locating users continue** to cause much debate over **how to apply jurisdictional limitations** to cyberspace.
- Indeed, the borderless nature of the Internet can, in theory, lead to **substantial overlap of laws** and **ambiguity** in their application.
- So what laws should govern an Internet user? **What jurisdiction should apply** to disputes arising from the use of the Internet, particularly at a time when local, state, national, and foreign authorities are claiming more expansive roles and asserting broader reach across cyberspace?

# Introduction (cont...)

Always A Pioneer, Always Ahead

- Despite the development of substantial caselaw on this issue since the early boom years of the Internet, these questions continue to be critically important when we consider that the protections afforded to intellectual property still vary among jurisdictions.
- With new technological tools such as **software-as-a-service solutions, cloud computing, and mobile applications**, and the increasing stealthiness of infringers, give added urgency to answering these questions with more certainty than in the past.

# Introduction (cont...)

- For example, in 2000 the Love Bug virus, which was launched from the Philippines, infected computers in at least twenty countries. Four years later, the Sasser worm “crippled computers worldwide.”
- Spammers and other online scammers currently ignore national borders, sending solicitation emails to potential victims in a host of countries.
- The **transnational nature of cybercrime challenges traditional conceptualizations of criminal jurisdiction** because conduct no longer necessarily occurs entirely within the territory of a single sovereign. A cybercriminal operating out of the United States can attack victims in the United States, in Germany, in Japan and other parts of the world with equal ease. **Cyberspace and computer technology make geography irrelevant.**

# Introduction (cont...)

This has several consequences for criminal jurisdiction:

- Jurisdiction may be completely lacking. In the previous example, assume that neither the United States nor any of the countries hosting victims of the hypothesized cybercriminal can assert jurisdiction over his conduct.
- Jurisdiction may exist but be impossible to assert. In the previous example, assume that the activity the hypothesized cybercriminal conducts from the United States is legal there but has been outlawed in Germany. Germany wants to prosecute the perpetrator for violating its laws; under established principles of criminal jurisdiction, Germany has the authority to prosecute him. The United States, however, refuses to turn him over to German authorities for prosecution because his conduct did not violate U.S. law.
- Jurisdiction may be claimed simultaneously by more than one country. This would mean, in the example given above, that the United States, Germany, Japan and one or more other countries all assert jurisdiction to prosecute the hypothesized cybercriminal. Here, the problem is one of establishing priorities, of deciding which country should be given the first opportunity to prosecute him, which should be given the next chance, etc.

# Sovereignty

- “sovereignty” is “a state’s lawful control over its territory...to the exclusion of other states, authority to govern in that territory, and authority to apply law there.”
- A sovereign can therefore prescribe what behaviors are acceptable within its territory, adjudicate claims that persons in its territory violated these prescriptions and punish them for their non-compliance. The principle developed, therefore, that “the character of an act as lawful...must be determined wholly by the law of the country where the act is done.”
- It followed from this that no sovereign could apply its criminal laws to conduct that took place in the territory of another sovereign.





# Jurisdiction: definition

- Jurisdiction under public international law is generally defined as:
  - “the government’s right under international law to regulate conduct in matters not exclusively of domestic concern”.
  - “the government’s general power to exercise authority over...persons and things”.
- Jurisdiction defines three kinds of power:
  - The power to prescribe
  - The power to adjudicate
  - The power to enforce

# The power to prescribe

- Relates principally to the power of a sovereign authority to establish and prescribe criminal and regulatory sanctions.
- to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things.
- A sovereign can prescribe law regarding:
  - a) conduct that occurs, in whole or in part, in its territory,
  - b) the status of persons in its territory, and
  - c) interests in things in its territory.
- Prescriptive jurisdiction can also extend beyond territory: A sovereign can prescribe laws that encompass:
  - a) conduct outside its territory that is intended to have a substantial effect within its territory,
  - b) the interests or status of its citizens outside its territory, and
  - c) conduct by non-citizens that occurs outside its territory but is directed at its interests.

# The power to adjudicate

- Relates to the power of the sovereign authority to subject persons or entities to the process of its courts or administrative tribunals in order to determine if its laws have been violated.
- A sovereign can subject persons to the adjudicative processes of its tribunals if the relationship between the sovereign and the person for whom adjudication is sought is “such as to make the exercise of jurisdiction reasonable.”
- A sovereign’s exercise of adjudicative jurisdiction is deemed to be reasonable if the person:
  - a) is present in its territory,
  - b) is domiciled or resides in its territory, or
  - c) carries on business or other activity in its territory.
- Adjudicative jurisdiction also extends beyond territory: A sovereign can legitimately adjudicate if the person: 
  - a) is its citizen, 
  - b) has consented to its exercise of jurisdiction, or
  - c) carried on activity outside its territory that has a “substantial, direct, and foreseeable effect” within its territory.

# The power to enforce

- Relates to the power of a sovereign authority to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgements.
- A sovereign can enforce its laws if it has jurisdiction to prescribe.
- A sovereign state cannot, however, enforce its criminal law in the territory of another state without that state's consent. The territorial character of jurisdiction to enforce is seen most clearly in the impermissibility...of extraterritorial police powers: the police of one state may not investigate crimes and arrest suspects in the territory of another state without that other state's consent. It is also reflected in the judicial sphere: the criminal courts of one state may not, as of right, sit in the territory of another...
- A sovereign can enforce its laws against someone who is located outside its territory by proceeding with a trial in absentia if it has jurisdiction to adjudicate and if it gives the person notice of the claims and an opportunity to be heard in advance of enforcement.



# The power to enforce

- Relates to the power of a sovereign authority to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgements.
- A sovereign can enforce its laws if it has jurisdiction to prescribe.
- A sovereign state cannot, however, enforce its criminal law in the territory of another state without that state's consent. The territorial character of jurisdiction to enforce is seen most clearly in the impermissibility...of extraterritorial police powers: the police of one state may not investigate crimes and arrest suspects in the territory of another state without that other state's consent. It is also reflected in the judicial sphere: the criminal courts of one state may not, as of right, sit in the territory of another...
- A sovereign can enforce its laws against someone who is located outside its territory by proceeding with a trial in absentia if it has jurisdiction to adjudicate and if it gives the person notice of the claims and an opportunity to be heard in advance of enforcement.

# Types of cybercrime

Always A Pioneer, Always Ahead

- In analyzing the extent to which existing jurisdictional principles can accommodate cybercrime the first step is to distinguish between two types of cybercrime:
  - Local cybercrime
  - Transnational cybercrime.

# Local cybercrime

Always A Pioneer, Always Ahead

- Conforms to the traditional model of crime because the commission of the cybercrime effectively takes place entirely within the territory of a single sovereign. In this type of cybercrime, both the perpetrator and the victim are physically in the sovereign's territory when the conduct constituting the offense is committed, so the "harm" to the victim is inflicted on the sovereign's territory.
- Cyberstalking is a good example of local cybercrime: The perpetrator and victim usually reside in the same community and know each other from encounters in the real-world; the perpetrator, who has become disgruntled for whatever reason, stalks the victim online, in an effort to conceal his identity and avoid apprehension. Although the perpetrator vectors his stalking activity through cyberspace, he and his victim are in the same localized area during the commission of his criminal activity.

# Transnational cybercrime

- In 1995, the United Nations (UN) defined transnational crime as offences “whose inception, perpetration and/or direct or indirect effects involve more than one country” (UNODC, 2002, p.4).
- Therefore, we can say that transnational cybercrime is cybercrime whose inception, perpetration and/or direct or indirect effects involves more than one country.
- In 2000 the UN Convention on Transnational Organized Crime defined an offence as transnational if it met one of these four conditions: if it is committed in more than one state, if it is committed in one state but a substantial part of its preparation, planning, direction, or control takes place in another state, if it is committed in one state but involves an organized criminal group that engages in criminal activities in more than one state, and finally, if it is committed in one state but has substantial effects in another state.



# Cyberspace as a criminal tool

Always A Pioneer, Always Ahead

- Cyberspace offers several distinct advantages as a criminal tool:
  - As the hypothetical stalker realized, it can provide a more reliable guarantee of anonymity than comparable tools, such as the post or the telephone.
  - It vastly increases the scale on which crimes are committed; a real-world criminal can defraud one victim at a time, but a cybercriminal can simultaneously defraud hundreds or even thousands of victims.
  - It allows crime to be automated; the real-world fraudster must personally commit his crime, but his cyber-counterpart lets automated systems carry out his frauds.
  - The characteristic that is most relevant to this discussion, however, is the ability to commit crimes remotely.

# Issue of transnational cybercrime

Always A Pioneer, Always Ahead

- As noted earlier, cyberspace makes physical space and sovereign boundaries irrelevant. This eradicates the need for offender-victim proximity and thereby creates new opportunities for criminals.
- A criminal operating out of, say, Nigeria, can use cyberspace defraud thousands of victims in countries around the world. The remote nature of the Nigerian perpetrator's crimes can create tremendous challenges for law enforcement officials as they attempt to identify and apprehend him.
- Although it may seem, at first glance, that the activity should prove equally challenging for the application of jurisdictional law, that may not be the case. The discussion of local cybercrime pointed out that it does not challenge jurisdictional law because it conforms to the traditional model of crime: all the elements of the offense occur in a single sovereign territory.
- This is certainly the simplest, most traditional instance in which a sovereign can exercise jurisdiction over an offense and an offender, but it does not exhaust the possibilities.

# Issue of transnational cybercrime

Always A Pioneer, Always Ahead

- Assume the Nigerian perpetrator defrauded individuals in Australia. While he was not in Australia when he committed these crimes, the country can assert jurisdiction over him under either of two theories.
- One theory is that part of the conduct involved in the commission of the offense occurred in Australia. Jurisdictional principles let a sovereign exercise jurisdiction when all or part of the conduct involved in the commission of an offense occurred in its territory. Australian prosecutors can argue that part of the conduct constituting the offense was committed in Australia because the actual victimization – the processes of persuading the victim to send money to the perpetrator and the actions the victim took to that end – occurred in the territory of Australia. This proposition has been accepted with regard to real-world crimes, and so it should succeed in this context.
- The other theory is that the perpetrator engaged in conduct outside Australia that was intended to (and did) have a substantial effect in its territory. The “substantial effect” is the victimization of Australian citizens; courts have accepted such victimization as the basis for a sovereign’s exercising jurisdiction over conduct occurring outside its territory. Since this perpetrator victimized more than one citizen of Australia, prosecutors could cite the cumulative effect of his activity to support their claim that his conduct had an effect sufficient to warrant the exercise of jurisdiction by this sovereign.

# Issue of transnational cybercrime

Always A Pioneer, Always Ahead

- While cybercrime challenges law and law enforcement in many ways, the prospect that countries can exercise jurisdiction over transnational cybercrime is actually quite encouraging. It seems that many countries can assert jurisdiction over external perpetrators by employing the approaches outlined above, i.e., by predicating jurisdiction on the premise that at least part of the offense occurred in their territory or by construing the offense as extra-territorial conduct that had a substantial effect within the jurisdiction.
- The intrinsic adequacy of existing jurisdictional principles to encompass extraterritorial cybercrime presumably accounts for the fact that the Council of Europe's Convention on Cybercrime did not introduce new jurisdictional predicates for this type of criminal activity. Instead, the Convention relies primarily on **territoriality** as the basis for exercising jurisdiction over cybercrime; **nationality** of the perpetrator is included as a secondary predicate.
- **Countries can**, of course, **adopt specialized jurisdictional statutes targeting cybercrime**. Some American states have done this. Arkansas, for example, has adopted a statute which states that "[f]or the purpose of determining jurisdiction," over cybercrime, **"a person is subject to prosecution in this state...if the transmission that constitutes the offense either originates in this state or is received in this state."**

# Issue of transnational cybercrime

Always A Pioneer, Always Ahead

- Hawaii and Oklahoma take a slightly different approach. Their cybercrime jurisdiction statutes state that one “who causes, by any means, the access of a computer...or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer...or computer network in each jurisdiction.” Ohio’s general criminal jurisdiction statute declares that the state has jurisdiction when someone “by means of a computer, computer system, computer network, telecommunication, telecommunications device, telecommunications service, or information service, causes or knowingly permits any writing, data, image, or other telecommunication to be disseminated or transmitted into this state in violation of the law of this state.”
- For some reason, West Virginia has one of the world’s most expansive cybercrime jurisdictional provisions. It declares that one who violates West Virginia cybercrime law “and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources...or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state.”

# Issue of transnational cybercrime

Always A Pioneer, Always Ahead

- The few jurisdictions that have adopted these very expansive jurisdictional provisions presumably see them as a pre-emptive measure. West Virginia, for example, surely cannot mean to prosecute every cybercrime the commission of which resulted in signals passing through the state; the purpose must be to give the state expanded jurisdiction which can be used if and when a particularly egregious case arises that otherwise has little direct connection to the jurisdiction. It seems, then, that the issues we must confront with regard to cybercrime jurisdiction involve not a failure of jurisdiction, but, perhaps, an excess of jurisdiction. The next section takes up this issue.

# Conflicting jurisdiction

- Since cybercrime tends to transcend national borders, it follows that the activities of a cybercriminal are likely to result in the commission of crimes in multiple countries. If, for example, John Doe uses a version of the “419 email scam” to defraud victims in Country A, Country B and Country C, he will have committed a crime (fraud) against victims in each of those jurisdictions. As long as each country has penal law that criminalizes the use of a computer and email to perpetrate fraud and procedural law that authorizes the exercise of criminal jurisdiction, John Doe can be prosecuted by Country A, Country B and Country C.
- If all three countries want to prosecute Doe, this creates a positive jurisdictional conflict, i.e., a situation in which more than one country claims jurisdiction over a perpetrator based on the same general course of conduct. Since Doe defrauded victims in each of the three countries, Country A, Country B and Country C are not each seeking to prosecute him for the “same” crime. Instead, each seeks to prosecute him for specific crimes that were committed against its citizens as part of an ongoing course of online criminal activity. It therefore becomes necessary to prioritize their respective claims to exercise jurisdiction over Doe.



# Prioritizing jurisdictional claims

Always A Pioneer, Always Ahead

- Traditional sources offer little guidance on how to prioritize conflicting jurisdictional claims, and the Council of Europe's Convention on Cybercrime, which seems likely source of guidance, does not attempt to resolve the issue. Article 22 of the Convention merely states that **when several parties claim jurisdiction over the same offender or offense**, **"the Parties involved shall...consult with a view to determining the most appropriate jurisdiction for prosecution."**
- The Council of Europe provision is similar to that found in other treaties. For example, the United Nations Convention against Transnational Organized Crime states that if a party to the Convention learns that "one or more other States Parties are conducting an investigation...or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall...consult...with a view to coordinating their actions."
- According to one source, since "general international law has not established a priority system among...jurisdictional theories," the solution has traditionally been negotiation, which was a viable option because jurisdictional conflicts were rare.



# Prioritizing jurisdictional claims

Always A Pioneer, Always Ahead

- As conflicts become more common, negotiation is likely to be less satisfactory because it is time-consuming, and it offers very little in the way of predictability. Factors that provide some guidance on the predictability of outcomes are useful not only in resolving jurisdictional conflicts but in preventing them. If, say, Country A knows that its assertion of jurisdiction is likely to be lesser to an assertion of jurisdiction by Country B, Country A is less likely to pursue its claim.
- The next section suggests factors that can appropriately be considered in resolving positive jurisdictional conflicts. The factors were derived from:
  - (a) practical processes that have been used to resolve similar conflicts,
  - (b) standards articulated for use in resolving other types of jurisdictional conflicts, and
  - (c) certain distinctive aspects of cybercrime.

# Prioritizing jurisdictional claims

- The factors outlined next are not intended to be a mandatory set of conditions, each of which must be satisfied to establish jurisdictional priorities. They should instead serve as elements that structure the general assessment of whether it is “reasonable” to assign first prosecution priority to Country A, Country B or Country C in a particular instance.
- The factors are not necessarily to be given equal weight. Some may militate more heavily in favor of giving a country priority than others, in a specific case or in general. While it might be reassuring to have a hierarchical, ranked system of factors for use in this analysis, the fact-sensitive nature of the analysis makes this inadvisable.
- Finally, these factors are not intended to be exhaustive. Other factors that are relevant in particular instances should also be considered in resolving positive jurisdictional conflicts.
- The factors considered are:
  - a) Custody of perpetrator
  - b) Harm
  - c) Victim nationality
  - d) Perpetrator nationality
  - e) Strength of the case against perpetrator
  - f) Punishment
  - g) Fairness and convenience

# Place of commission of the crime

Always A Pioneer, Always Ahead

- A factor that has traditionally been important in resolving jurisdictional conflicts is “the place of commission of the crime.” The place of commission of the crime is useful in resolving jurisdictional conflicts that arise with regard to real-world crimes because they are, for the most part, crimes that occur wholly within a single jurisdiction. There is, therefore, only one “place” where the crime was committed.
- This is not true for the virtual world; as noted earlier, a cybercriminal can easily commit multiple offenses, almost simultaneously, in many countries. In the scenario given above, John Doe perpetrated distinct fraud offenses against victims who were physically located in Country A, Country B and Country C. Each of these countries can therefore legitimately claim to be the “place of the commission of the crime[s]” (against its citizens) because Doe did, in fact, commit cybercrimes “in” Country A, “in” Country B and “in” Country C.
- Because “the place of commission of the crime” is not a zero-sum phenomenon for cybercrime, this factor is unlikely to be particularly helpful in resolving positive jurisdictional conflicts. In the scenarios we have outlined, for example, it results in a wash: Each of the countries claiming jurisdiction is a “place of commission”

# Custody of perpetrator

- The most obvious, and perhaps most logical, factor to be considered in resolving jurisdictional conflicts is that a country has custody of the alleged perpetrator. One's presence within a jurisdiction is the most basic, most ancient, rationale supporting jurisdiction.
- Custody should play a rather more complex role in establishing jurisdictional priority with regard to cybercrimes than it does for real-world crimes. As noted earlier, competing claims to jurisdiction over real-world crimes tend to be predicated on the commission of a single offense or a single course of conduct that constitutes the commission of multiple offenses.
- Here, the issue to be resolved is which of several competing countries will be allowed to bring the individual to justice for the commission of that offense or course of conduct; the conflicts all focus on the same criminal activity. This means, in effect, that none of the competing countries actually "loses" if it is not given the first opportunity to prosecute the perpetrator; he will still be brought to justice for his role in the underlying criminal transaction. And that may well resolve the matter; the other countries which were competing to prosecute him may decide, once he has been convicted and sanctioned, that this is sufficient, that there is no reason for them to pursue sequential prosecutions.

# Custody of perpetrator

- In the cybercrime context, the jurisdictional conflicts focus on a perpetrator's committing discrete offenses against unrelated victims in each of the countries that is vying for the chance to prosecute him. Instead of each country's asserting a claim based on the same offense or course of conduct, each asserts a claim that is based upon a distinct, severable criminal transaction unique to that country; the transaction is the victimization of its citizens while they were in its territory. Since the criminal transactions are factually and legally severable, prosecution by one of the competing countries may vindicate its interest in protecting its citizens, but it does nothing to vindicate the other countries' interest in doing so. And the remote victimization typical of cybercrime gives countries a heightened interest in prosecuting those who exploit their citizens; such prosecutions symbolically attest to a country's commitment, and ability, to pursue justice for its citizens against this emerging and unprecedented threat.
- Assume that Max Schultz, a German national and a terrorist, hijacks a bus traveling from Barcelona to Cordoba and kills three of the passengers (a U.S. citizen, a citizen of Japan and a citizen of Ireland) before he is apprehended. Spain wants to prosecute Schultz for hijacking the bus, killing three passengers, jeopardizing the safety of the other passengers and terrorism. The United States, Japan and Ireland each wants to prosecute him for killing their citizen, so we have a positive jurisdictional conflict.
- Logically, the fact that Spain has custody of Schultz (coupled with the fact that he committed his crimes in Spain) weighs heavily in favor of giving Spain the first opportunity to prosecute. If Spain were to prosecute, convict and impose a suitable penalty upon Schultz, the other countries might decide this outcome was sufficient, and not pursue their own prosecutions.

# Custody of perpetrator

Always A Pioneer, Always Ahead

- Now assume Schultz is a cybercriminal who victimized citizens of Ireland, Japan, Spain and the United States by conducting an online fraud scam from his apartment in San Francisco. Assume that he defrauded 10 victims in Ireland, 15 in Japan, 25 in Spain and 15 in the United States, and that U.S. officials have him in custody. U.S. authorities want to prosecute Schultz for victimizing U.S. citizens; Ireland, Japan and Spain each want to prosecute him for victimizing their citizens. In resolving the jurisdictional conflict, how much weight should be given to the fact that the U.S. has Schultz in custody? One factual circumstance that differentiates this scenario from the first scenario is the relationship between custody and the criminal transaction. Like Schultz-the-terrorist, Schultz-the-cybercriminal committed crimes “in” the country that has him in custody.
- But unlike Schultz-the-terrorist, Schultz-the-cybercriminal also victimized citizens of three other countries while they were in their own countries, and he was in the United States. His being in the United States seems coincident, a matter that is factually and logically irrelevant to the crimes he committed. The U.S. has custody of him because he happened to choose that country as the situs for his fraud operations. Unlike the Schultz-as-terrorist scenario, there is no inherent factual or logical relationship between Schultz’s criminal conduct and his being in the United States.

# Custody of perpetrator

Always A Pioneer, Always Ahead

- It therefore seems appropriate to use a “custody-plus” standard. Under this approach, the United States’ claim to jurisdictional priority would be strengthened if it demonstrates that it acquired custody of Schultz as the result, say, of intensive investigatory efforts that resulted in his being apprehended when he might otherwise have escaped official notice. Such an effort reasonably supports the inference that U.S. officials were dedicated to pursuing justice in this case and were willing to devote substantial resources to tracking him down and apprehending him. Under a “custody-plus” standard, the U.S’ claim to jurisdictional priority would be eroded if it acquired custody of Schultz through inadvertence. This does not mean that its custody of Schultz would play no role in the jurisdictional prioritization analysis; it means it would be given less emphasis than if its custody of Schultz were the result of affirmative efforts to locate and secure him.

- The scenario outlined above suggests another factor that should be considered in resolving positive jurisdictional conflicts: the “harm” the perpetrator inflicted upon those seeking to prosecute him. To incorporate “harm” into the jurisdictional calculus, it is necessary to identify indicators of “harm”—metrics that can be used to assess the relative extent to which each jurisdiction has been injured by the perpetrator’s activities.
- An obvious measure of “harm” is the number of victims. In the scenario given above, the “harm” Schultz-the-cybercriminal inflicted in each jurisdiction is essentially equivalent in terms of the number of victims: He defrauded 15 people in the United States, 10 in Ireland, 15 in Japan and 25 in Spain. This indicator is therefore of little assistance in resolving the jurisdictional conflicts in this instance, but it may be more helpful in other cases.
- Assume that cybercriminal Doe creates and releases a computer virus which spreads unevenly among a number of countries. Assume that the Doe virus inflicts “harm” (loss of computer files, computer services and similar injuries) upon (a) 2 million victims in the United States, (b) 100,000 victims in France and (c) 150 victims in Japan. If we use the number of victims as an indicator of “harm” resulting from Doe’s efforts, then “harm,” in this instance, would weigh toward giving the United States first priority, followed by France and then by Japan.



- The utility of using “harm” as a factor in this analysis might be enhanced if it included an assessment of precisely “how much” each victim was injured. The most objective indicator of “how much” a victim was injured is the extent of the victim’s monetary loss. Monetary loss can encompass not only the funds a cybercriminal defrauded, extorted or stole from victims. It can also encompass “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, system, or information to its condition prior to the offense, and any revenue lost, or other consequential damages incurred because of interruption of service.”
- Monetary losses would provide a benchmark for the precise level of injury inflicted on each individual victim; it would also provide an indicator of the collective “harm” Schultz inflicted in each country. So, assume that in the Schultz scenario the victims (a) in the United States lost a total of \$2 million dollars, (b) in France lost a total of \$10 million and (c) in Japan lost a total of \$3 million. When “loss” is factored into the analysis, “harm” would weigh toward giving France first priority, followed by Japan and then by the United States.
- Using victim numbers and monetary losses as indicators of “harm” is satisfactory for the more routine cybercrimes. Other types of cybercrime, such as economic espionage, also inflict systemic “harms.” Incorporating the “harm” caused by economic espionage into the jurisdictional prioritization analysis would require articulating some metric that could be used to quantify the “harm” resulting from the offense.
- Much the same will be true for cybercrimes that are committed for other than economic reasons. This category of cybercrime would encompass attacks on national infrastructures, on medical and educational facilities and government computer systems.

# Victim nationality

Always A Pioneer, Always Ahead

- The cybercrime scenario postulated earlier assumed John Doe, the fictive cybercriminal, committed crimes in each of the countries seeking to prosecute him (Countries A, B and C). It does not, therefore, seem that victim nationality is a particularly significant factor in resolving the jurisdictional conflicts that result from his activities.
- It is reasonable, first, to assume that some, if not all, of the offenses he committed in each country were directed at citizens of that country who were “in” the country at the time. As with the “place of commission of the crime,” this puts the three claimant countries in a position of equivalence; each has citizens who were victimized by Doe. Victim nationality is therefore of little value in resolving the jurisdictional conflicts.
- If Doe somehow managed to commit cybercrimes in each of the countries but managed to victimize only those who were not citizens of that country, victim nationality would still be of little value in resolving the jurisdictional conflicts. We derive this conclusion from the following premise: It should be irrelevant to Country A that John Doe victimized citizens of Country B while they were located within the territory of Country A; since John Doe’s victimization of non-citizens of Country A was, in effect, an attack on Country A’s sovereignty, it should not matter to Country A whether the individual targets of the attack were its own citizens or resident aliens.
- There is a residual category in which victim nationality can become an issue: John Doe victimizes a citizen of Country A while that person is in Country B. For real-world crimes, this scenario can generate a compelling desire on the part of national officials to prosecute those who victimized their citizen while she was abroad. This is not, however, a significant issue in the context of cybercrimes.

# Victim nationality

Always A Pioneer, Always Ahead

- Cybercrime victimization is empirically more likely to occur while someone is at work or at home in their own country. Even if someone is victimized online while they are in another country, the victimization is likely to occur while they are utilizing computer resources that are physically located in their own country. If an American citizen, were victimized by an online fraudster while traveling in Spain, the consummation of the fraud would be predicated upon the use of credit card and/or banking facilities that are physically located in the United States.
- Also, while online victimization can inflict financial and, perhaps, psychological, “harm,” it does not produce the type of physical harm that gives rise to the compelling desire noted above. When a citizen of Country A is killed or severely injured by a criminal in Country B, Country A may seek to prosecute the Country B perpetrator because it believes this demonstrates its commitment to protecting its citizens’ physical safety even when they are abroad. So far, individual safety has not been jeopardized by cybercrime, which suggests that this commitment is unlikely to play an important role in assertions of cybercrime jurisdiction.

# Perpetrator nationality

Always A Pioneer, Always Ahead

- In the context of real-world crime, nationality is a factor that militates in favor of awarding jurisdictional priority. In the cybercrime context, it seems perpetrator nationality should operate as an inverse factor, i.e., as a factor that militates against, rather than for, the assertion of jurisdiction.
- To understand why this is so, consider the original scenario set out above, in which Doe commits discrete cybercrimes against citizens of Country A, Country B and Country C. Assume Doe is a citizen of Country A which, like the other countries, seeks to prosecute him. Factually, Doe's citizenship does give him a unique connection to Country A; this, alone, might suggest that Country A be given priority. Logically, however, Doe's citizenship should weigh in favor of giving first priority to Country B and Country C (in whatever order is dictated by a consideration of other factors), and reserving Country A for last.
- This conclusion is based on the premise that since Country A's citizen victimized citizens of Country B and Country C, those countries should be given the initial opportunities to exact justice from him. Country A is, in a pragmatic, empirical sense, "responsible" for what Doe has done; that is, he is a "product" of Country A and, at least in a symbolic sense, Country A can be said to have "allowed" him to prey on citizens of other countries.
- As one scholar noted, "nationality-based criminal jurisdiction reflects the need [for one state] to maintain good relations with other states...by deterring conduct by its own nationals that reflects poorly on the state abroad."

# Perpetrator nationality

- Historically, the concern has been with a citizen who commits crimes while in another country and then returns home; the goal has been to ensure that the offender's own country does not shield him from justice by declining to prosecute him or to extradite him. The principle of “aut dedere, aut iudicare” (‘to hand over, or to bring to trial’), which was incorporated into the Convention on Cybercrime, was developed to address this possibility.
- The “aut dedere” principle, and the assumption that nationality is a factor that weighs in favor of awarding jurisdictional priority, both assume traditional, real-world crime. That is, they assume a scenario in which John Doe, a citizen of Country A, travels to Country C, commits a crime against one of its citizens while he is there, and then returns to Country A. Both Country A and Country C want to prosecute Doe; the “aut dedere” principle gives Country A the option of handing Doe over to Country C for prosecution or prosecuting him itself. Assume, that Country A has jurisdiction over the conduct at issue and can prosecute Doe for the crime he committed in Country C. This creates a positive jurisdictional conflict. Under the traditional analysis, Doe's nationality weighs heavily in favor of giving priority to Country A. The generally articulated rationale for this is the strength of the factual and legal link between Doe and Country A. This deference is also implicitly predicated on the proposition noted earlier, i.e., that Country A is, in effect, “responsible” for its citizen's criminality. This proposition has on occasion been made explicit with regard to real-world crime; one notable instance is efforts to combat sex tourism, which encourages “sending countries” to prosecute their nationals who travel abroad for the purpose of having sex with children.

# Perpetrator nationality

Always A Pioneer, Always Ahead

- Efforts to combat sex tourism encourage countries to prosecute their nationals both because of the recognition that the countries are “responsible” for the crimes of their citizens and because of a concern that the receiving countries, the “place of commission of the crime,” may not seek to prosecute them. We, of course, are dealing with the converse situation: the scenario in which multiple countries are vying to prosecute a cybercriminal who has committed crimes “in” each country. The second issue noted above, i.e., lack of prosecution by “the place of commission of the crime,” is therefore inapplicable. This leaves the premise that a state should be given first preference to prosecute its citizen for a real-world crime committed abroad because it is “responsible” for the conduct of its citizens.
- To understand why the opposite should be true for cybercrimes, consider this example: Assume Doe is a citizen of the United States who used a rented office in San Jose, California to commit cybercrimes against citizens of other countries. Assume he successfully conducted a “419 fraud scheme” for over a year, and focused his efforts on citizens of other countries because he believed this would minimize his chances of being prosecuted in the United States. Assume, further, that Doe victimized (a) 100 citizens of England, (b) 200 citizens of South Korea and (c) 50 citizens of Brazil. Each of these countries seeks to prosecute him.
- Assume Doe can be prosecuted in the United States for his crimes against the citizens of these other countries and U.S. authorities are willing to prosecute him. Why should his nationality weigh in favor of giving the U.S. priority to prosecute? Since “the place of commission of the crime” is, in a non-zero-sum sense, in England, South Korea and/or Brazil, respectively, the U.S.’ only claim to priority is Doe’s nationality. Aside from that, it has no factual or legal connection to the offenses; its only connection with them is that its citizen victimized citizens of other countries, which hardly seems to warrant giving the U.S. priority.

# Perpetrator nationality

Always A Pioneer, Always Ahead

A crime is a transgression against a sovereign; it represents a breach of the sovereign's obligation, and ability, to ensure order within its territory. Historically, crime has been an internal matter; countries have been able to maintain order by controlling the behavior of those within the territory they control. Cybercrime challenges that ability; countries now have to deal with external threats from cybercriminals like Doe. His activities are an affront to the sovereignty of England, South Korea and Brazil; they in no way compromised the sovereignty of the United States. Indeed, as noted earlier, one can conclude that the U.S. is in a sense "responsible" for Doe's crimes: The United States did not encourage, facilitate or otherwise directly contribute to the commission of his crimes, but it did default on its obligation to deter criminality on the part of its own citizens, a default that resulted in "harm" to citizens of other countries. Logically, therefore, the injured sovereigns should be given priority over the non-injured sovereign; here, nationality should function as an inverse factor in the jurisdictional priority analysis.

The same conclusion holds if we modify the initial scenario so that Doe also commits crimes against citizens of the United States. The United States is now an injured sovereign, like England, South Korea and Brazil. But unlike those countries, the United States is, at least to some extent, "responsible" for Doe's criminality. The host country's defaulting on its obligation to control criminality by its citizens should still function as an inverse factor in the jurisdictional priority analysis; the "victim" sovereigns should be given preference over the host country.

# Strength of the case against perpetrator

Always A Pioneer, Always Ahead

- The strength of the case each country can bring should be a very important in resolving positive jurisdictional. In the scenario given earlier, the ultimate goal is to ensure Doe is brought to justice; it would therefore not be reasonable to give priority to Country A, which has a weak case against Doe, instead of to Country C, which has a very strong case against him.
- In making this determination, it is appropriate to consider not only the extent to which a country has collected evidence tying a suspect to the cybercrime(s) it wants to prosecute; the analysis should also consider whether the defendant may be able to raise objections to the use of this evidence and have it ruled in admissible. The analysis might also focus on related issues, such as the applicability of the statute of limitations or other defenses the defendant(s) might raise.



- The punishment that can be imposed upon conviction is a factor U.S. prosecutors often cite when multiple states seek to prosecute the same individual(s). The goal here should be to ensure just punishment, not to seek punishment for punishment's sake.
- To understand why this can be important, it is useful to consider a variation on the events surrounding the dissemination of the "Love Bug" virus. In May, 2000, the Love Bug virus appeared and spread around the world, causing billions of dollars in damage. Federal Bureau of Investigation agents pinpointed Manila as the source of the virus. FBI agents working with agents from the Philippines' National Bureau of Investigation identified Onel de Guzman as the person who was probably responsible for disseminating the virus. The agents searched de Guzman's home and discovered evidence linking him to the virus, but the Philippines had not, at the time, criminalized virus dissemination. De Guzman therefore could not be prosecuted in the Philippines or extradited for prosecution in the United States.
- Assume the Philippines criminalized the dissemination of a computer virus months before the Love Bug appeared. Assume three countries want to prosecute de Guzman for disseminating the Love Bug: the Philippines; the United States; and South Korea. Each has citizens who victimized by the Love Bug. Each can assemble a strong case that is based on admissible evidence and free from defenses de Guzman can invoke. The government of the Philippines "has" de Guzman, which works in their favor; but the effect of the Philippines' having custody of the alleged perpetrator is offset by his being a Philippine national.

- Though the Philippines has criminalized virus dissemination, it has made the crime a minor offense punishable by 2 weeks' imprisonment in a local jail and a fine equivalent to \$100. In the United States, disseminating a computer virus is punishable by up to 10 years imprisonment plus a fine of \$250,000. Assume South Korean law makes virus dissemination a felony punishable by up to 3 years in prison and a fine of \$5,000. Since the Love Bug inflicted millions of dollars in damage on citizens of these three countries, along with citizens of many other countries, it seems that the prosecution should have a certain gravitas, i.e., should result in the imposition of sanctions that might deter a similarly-situated individual from engaging in similar misconduct in the future. If one accepts that proposition, it seems reasonable to consider the punishment that can be imposed, if prosecution is successful; based on that factor, alone, it seems prosecution would be most appropriate in the United States or in South Korea.
- Here, the severity of the available punishment acts as a positive factor; countries that can impose more severe punishments are favored in the assignment of jurisdictional priority. But punishment can also play a negative role in determining the locus of prosecution; many countries, for example, will not extradite a murder suspect to the U.S. unless it agrees not to seek capital punishment. Regardless of the severity of the specific punishment that can be imposed in a given, the jurisdictional priority analysis should incorporate an assessment of the extent to which the punishment available in each of the claiming jurisdictions can be considered to be "too much" punishment, especially for the crime charged.

# Fairness and convenience

Always A Pioneer, Always Ahead

- Another factor that should be included in the calculus used to resolve jurisdictional conflicts in cybercrime cases is the anticipated fairness and impartiality of a prosecution in a given country. The analysis might also focus on the extent to which prosecution in a particular country would be convenient (or, conversely, inconvenient) for witnesses and others involved in the proceeding, and on the extent to which any possible inconvenience could be mitigated by allowing witnesses to testify remotely, via video.

# Summary

- Unlike other areas of cybercrime law, countries' ability to assert jurisdiction over those who perpetrate cybercrime, both locally and transnationally, does not seem to be particularly problematic. While some jurisdictions have adopted cybercrime-specific jurisdictional statutes, the basic principles that have been used to justify the assertion of jurisdiction over real-world criminals can also justify the assertion of jurisdiction over cybercriminals, both internal and external.
- The more difficult – and as yet unresolved – issue is **how to prioritize conflicting claims to assert jurisdiction over transnational cybercriminals**. This topic outlines factors that should be incorporated into the calculus used for this purpose. It is extremely important that nations agree on such a calculus to prevent cybercriminals' exploiting jurisdictional conflicts for their benefit.

# Thank You



[www.utem.edu.my](http://www.utem.edu.my)