Jurisdiction

In a previous presentation, we have seen that in the case of cybercrime, it may be difficult to establish that an arrest of a suspect is "lawful". A major factor underlying this difficulty is the problem of establishing the jurisdiction responsible for the investigation, prosecution, and trial of an offender. The concept of jurisdiction pertains to which agency or court has the authority to administer justice in a particular matter, and to the scope of those agencies' and courts' authority. Jurisdiction is usually based on the geographic location where the agencies and courts are located. We keep stressing that in cybercrime, the victim and the offender do not have to be in the same physical place at the same time. Cybercrime often takes place across borders- both state borders in the United States and national borders around the world. In a cybercrime attack, a victim may be in country A, while the offender is in country B; or the victims may be in countries B, C, and D. Beyond this, the offender may route the attack through computers in countries E, F and so on. Acts on the Internet that are legal in the state/country where they are initiated may be illegal in other states/countries, even if the act is not targeted at that particular state/country. There are also conflicts about jurisdiction, both negative (no state/country claims jurisdiction) and positive (several states/countries claim jurisdiction at the same time). Over all this, it is unclear just what constitutes jurisdiction: is it the place of the cybercrime act itself, the state/country where the perpetrator resides, the location where the effect was felt, or the nationality of the computer user that is under attack? Or all of these at once? It turns out that countries think quite differently on this issue. The cybercrime statutes of numerous countries show varying and diverging jurisdiction clauses. This makes it very hard to determine "where" the cybercrime occurred; if this fact cannot be definitively established, it is problematic to establish who (which state/country) has jurisdiction in the case.

There is no universally agreed upon standard for determining jurisdiction in a criminal case.
There are certain principles used by countries to claim jurisdiction.

1) Territoriality: A nation may claim jurisdiction if a crime, or any element of a crime, took place within its territorial boundaries.
2) Effects: A country may claim jurisdiction of crime committed anywhere if it produces substantial effects on its own territory
3) Nationality: A country can claim jurisdiction over its own citizens who commit crime anywhere or in cases where foreign nationals commit crime against its citizens in another country.
4) Protective: A country may claim jurisdiction in cases where crime is committed abroad but threaten the country's national security.
5) Universality: This principle applies to certain types of crimes, such as war crimes, crimes against humanity, and maritime piracy wherever they take place.

These principles are applicable both in cases of traditional/terrestrial crime and cybercrime.

If and/or when a suspect has been identified, there is a question of extraditing the suspect from one jurisdiction to another. Extradition is the formal process of one nation/state surrendering an individual to another nation/state for prosecution or punishment for crimes committed in the requesting nation/state's jurisdiction. Internationally, it is typically enabled by a bilateral or multilateral treaty.

Extradition laws give a nation the authority to hand over someone to another nation for purposes of criminal trial or punishment. Whether someone can be extradited depends on the laws of the nations involved and whether there is an extradition treaty in place. Extradition can also take place within the United States in a state-to-state extradition.

An extradition treaty is an agreement between two countries to extradite to each other persons who've been charged or found guilty of an extraditable offense. The United States has extradition treaties with more than 100 countries as well as with the European Union. However, it does not have extradition treaties with 70 countries, including Russia and China.

Extraditable offenses generally include crimes that are punishable in both countries by at least one-year imprisonment- that is, felonies. A felony is a serious crime that is usually punishable by a prison term of at least one year. (Misdemeanors are less serious crime, carrying penalties of incarceration for less than a year and/or a monetary fine.) These offenses include the attempt or conspiracy to commit an extraditable offense. Special inclusion for extraditable offenses are matters that involve taxes, custom duties, and foreign exchange offenses. The reason for this is that, as will be described below, the process of extraditing a suspect/felon between countries is typically complex and expensive.

The treaties often exclude the extradition of a citizen of the requested state. For instance, the United States will not, in most cases, extradite one of its own citizens to another country.

There are other scenarios where extradition can be refused. Many nations may refuse to extradite people who may face torture or the death penalty in the requesting nation.

When the United States wants to extradite someone who is residing in a foreign country with an extradition treaty, a complaint is filed in any U.S. court stating the charges and the treaty requirements. A warrant for the persons apprehension will be prepared and given to the Secretary of State who will then contact the foreign government to begin the international extradition process.

The receiving nation then looks to its treaty obligations to the requesting nation and to its own laws on extradition, and decides whether or not to extradite. Many nations do not extradite individuals for certain political crimes. These can include treason, sedition, espionage and alleged crimes relating to criticism of political leaders.

In countries with no extradition treaty with the United States, it's still possible to extradite someone. In these cases, the United States must negotiate with the non-extradition treaty country, but they can say no.

The introduction and widespread adoption of cloud computing has complicated the issue of jurisdiction in cybercrime cases even further. Cloud computing may be defined as the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing allows users- both businesses and individuals- to share data, collaborate on projects, and generally work more efficiently and productively. There are also disadvantages to using the cloud for data processing: it requires a connection to the Internet (with all of the attendant threats and attacks that come with connectivity); it means that the user- whether a business or individual- loses some control over his/her/its own data; not all cloud computing host servers provide the same level of service; and, if there are any technical issues which arise, the user is forced to contact and deal with the host of the cloud service. But, perhaps the biggest disadvantage of cloud computing is the threat of security breaches- i.e. cybercrime. And here is the jurisdictional problem: Since the data are stored, managed, and processed on remote servers that are geographically scattered in multiple locations, it isn't always clear where the data are in the first place. If there is evidence of a cybercrime involving data in a cloud network, distributed over several jurisdictions, to which jurisdiction does law enforcement petition for authority to conduct a search?

In spite of the difficulties and problems in defining and establishing jurisdiction in cases of cybercrime, there have been some successful investigations. The next slide presents a table of these successes, with a brief description of the form of cybercrime investigated.

Investigation Code Name	Cybercrime Investigated
Operation Cathedral	**Operation Cathedral** was a police operation that broke up an international ***child pornography*** ring called The *Wonderland Club* operating over the Internet. It was led by the British National Crime Squad in cooperation with 13 other police forces around the globe, who arrested 107 suspects across 12 countries on September 1, 1998.
Operation Buccaneer	**Operation Buccaneer** marks the most significant law enforcement penetration to date of international organizations engaged in ***the illegal distribution of copyrighted software, games and movies*** over the Internet. The enforcement action involved the simultaneous execution of 58 search warrants against high-level "warez" leadership and members within the United States and abroad. It was also the first transnational enforcement action to strike at the most highly placed and skilled members of these international criminal enterprises.
Operation Artus	**Operation Artus** the seizure of computers and videos as part of an international raid to break up a ***child pornography*** ring. Search warrants were issued in the United Kingdom, Canada, France, Germany, Switzerland, Spain, Japan, Finland, Austria and Sweden. Customs said that a common aim of members of this group was to find and exchange child pornography in DVD quality movie file format. As a requirement members had to offer new child pornography material to remain part of the group.
Operation Falcon	**Operation FALCON** (**Federal and Local Cops Organized Nationally**) is the name of several week-long dragnets organized by the United States Marshals Service. FALCON I occurred between April 4 and April 10, 2005 (also Crime Victims' Rights Week), FALCON II during the week of April 17-23, 2006, and FALCON III from October 22-28, 2006. More than 35,000 fugitives across the United States were arrested … as part of an annual sweep that teams the U.S. Marshals Service with local law enforcement in a … push to clean up the streets, U.S. Marshals said Thursday.

Operation Delego	**Operation Delego** is a major international law enforcement investigation launched in 2009, which dismantled an international ***pedophile*** ring that operated an invitation-only Internet site named Dreamboard which featured incentives for images of the violent sexual abuse of young children under twelve, including infants.
Silk Road	**Silk Road** was a digital black market platform that was popular for hosting ***money laundering*** activities and illegal ***drug transactions*** using Bitcoin. Silk Road, regarded as the first internet darknet market, was launched in 2011 and eventually shut down by the FBI in 2013. The Silk Road came to its demise in 2013 after the FBI, after learning about the existence of the hidden marketplace, colluded with the DEA, IRS, and Customs agents. Although the federal agents admitted that the use of Tor and Bitcoin to obscure addresses were major obstacles that they encountered, they were still able to crackdown on the underground drug market. The FBI shut down the site permanently, seized more than 144,000 Bitcoins (then valued at $122 million), and arrested a number of users of the site.