

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

Panel: Cybercrimes and the Domestication of International Criminal Law

*Professor Jordan Paust, Panelist**

Many issues concerning transnational cybercrimes relate to international law, with respect to issues such as jurisdiction, searches in the United States and abroad, and more. With respect to cybercrime, it seems that there is no universally agreed upon definition. It may not be necessary to have a definition, but the phrase is used quite often. Some identify two basic types of cybercrime: computer crimes and computer related crimes where a computer is used for some other type of international or domestic crime.

With respect to computer crime, the targeting of personal computers or computer systems or networks has implications regarding cyberspace jurisdictional issues. For example, one could target the security of a system or a network through such tactics as breaking down security, computer breakdowns, halting or disrupting use, blocking use, entry into computer systems or actual computers through worms and viruses, and vandalism

Another type of targeting could involve targeting data stored or processed information through methods such as espionage, impermissible mining of data, stealing of data through means such as identity theft, stealing access codes or encryption keys, and destroying or altering data for various purposes.

Computer-related crime can involve misuse of computer systems or networks for international or domestic crimes, and each misuse might implicate different aspects of jurisdiction under international law. For example, misuse of a computer network for crimes under customary international law will implicate universal

* Jordan Paust is the Mike and Teresa Baker Law Center Professor at the University of Houston. Professor Paust has been a visiting professor at a number of schools both inside and outside the United States. His books include *International Law and Litigation in the U.S.* (West Group, 2nd ed. 2005); *International Law as Law of the United States* (Carolina Academic Press, 2nd ed. 2003); and *International Criminal Law: Cases and Materials* (Carolina Academic Press, 3rd ed. 2007).

jurisdiction. Such crimes can be committed through use of computer networks or systems to facilitate terrorism, to facilitate drug trafficking, to facilitate trafficking in people, or for money laundering, theft or fraud. One common example is the use of e-mails promising money in exchange for an account number, password and/or a person's birthdate. Misuses may be engaged in with respect to various domestic or international crimes, including gambling, hate speech, and pornography.

It should also be noted that cybercrime in some contexts has been mischaracterized. For example, most types of cybercrime are not terrorism. Since 1985, the United Nation's General Assembly and Security Council have passed resolutions condemning all forms of terrorism, for any purpose, by any person, as a crime under international law over which there is universal jurisdiction.¹ There is no widely agreed upon definition of "terrorism." However, from an objective point of view, terrorism must involve an intentional tactic or strategy to produce a terror outcome in a targeted group. If we are looking at terrorism for political purposes as opposed to use within organized crime, other elements can be added.² In addition, there must be an intent to produce a terror outcome. Sometimes computer hacking, such as hacking into classified data, is not necessarily terroristic in purpose or effect.

Cyber-attacks are also sometimes mischaracterized as armed attacks triggering the right of armed use of force in response under the United Nations Charter Chapter VII, "Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," Article 51.³ But clearly some cyber-attacks can be significant, very injurious, and create serious national security threats. However, a cyber-attack simply does not involve an armed attack or the use of armed force. Therefore, the responsive action can be more limited than that allowed under Article 51 of the UN Charter, which allows the right of self-defense in case of an "armed attack."

With respect to permissible types of computer systems or network interferences, the permissible use of a cyber-attack in self-defense can occur when one is engaged in legitimate self-defense against an armed attack by a group like Al-Qaeda.

1. See, e.g. G.A. Res. 40/61, U.N. Doc A/RES/61 (Dec. 9, 1985); JORDAN J. PAUST, M. CHERIF BASSIOUNI, *et al.*, INTERNATIONAL CRIMINAL LAW 827, 841, 844 (3rd ed. 2007) [hereinafter ICL].
2. See, e.g., ICL, *supra* note 1, at 832-36, 841-43.
3. U.N. Charter art. 51, available at <http://www.un.org/aboutun/charter/index.html>.

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

As a hypothetical, if Al-Qaeda had a computer system, the United States would like to know about that. As part of a lawful responsive action by the United States against a non-state actor group, if Al-Qaeda was engaged in ongoing processes of armed attack, the United States could target Al-Qaeda's computer network.

Also, during armed conflicts against a state enemy, the targeting of military targets is permissible, and includes targeting of computer networks or systems that a military command structure would be using to support its war effort. Power grids and communication networks used by the military might also be disrupted, but there are potential problems concerning the effects on civilians. In such contexts, we must apply principles of international law that are not self-applicative, such as general principles of necessity and proportionality concerning targets and targeting.

Permission of the state containing the target is not required. However, some disagree about this if a non-state actor leads an armed attack against the targeted state. For example, if we have an Al-Qaeda type group in Pakistan, and the United States is still under a process of armed attack due to attacks on United States embassies in Tanzania and Kenya, the attack on the USS Cole, and the 9/11 attack, there is debate regarding whether the United States could target the group without Pakistan's permission. Under Article 51 of the Charter, a state can respond with military force against non-state actor attacks, such as Al-Qaeda, as long as the process of armed attack is ongoing, with no significant lulls, and in that case the state has not engaged in reprisal actions (which are impermissible).

Although a number of states disagree, especially throughout Latin America, the majority approach is that a state can respond with military force against non-state attackers located in a foreign state without foreign state consent.⁴ For example, the United States could target Bin Laden in Pakistan without Pakistani consent. However, that does not mean that the state might not have foreign affairs problems such as diplomacy concerns.

If a state is involved in a war, most would agree that the state could disrupt an enemy's computer capability. For example, a lot of United States troops on the battlefield in Iraq carry personal computers, and the system is targetable.

4. See, e.g., ICL, *supra* note 1, at 451-52, 603.

*Question Posed by Elena Duarte, Fellow Panelist**

How do you think that would play out in the United States, given things like the warrantless wiretapping?

Jordan Paust: There are privacy interests involved. But people should expect that their email can be monitored. The expectation test here involves the reasonable person standard. If you accept the premise that Al-Qaeda is engaged in a continual process of armed attacks and they have a sleeper group in the United States that has a computer system designed to help disrupt the United States' national security computer systems, can the United States respond, even preemptively? I am not talking about Article 51 preemptive use of force now, because we are addressing a disruption in the United States and it is more of a law enforcement responsive action. However, I do not see it as applying only to law enforcement. If we are talking about a context of ongoing processes of armed attack, the disruption would arguably fit within an Article 51 self-defense response, which is authorized by law, and I have limited it to Al-Qaeda networks, I am not going to creep into data mining and other issues involving U.S. citizen computers and systems which are much more problematic.

Choice points are aspects of fact that require us to make a choice about how law would be applied. Although it is a really significant concern currently, I did want to stop with ongoing process of attack, during which a state wants to disrupt an enemy system in an anticipatory self-defense.

We have to rethink some types of international law as they apply in our domestic legal process. This president is bound by the law of war and bound by the treaty law of the United States.⁵ The president is also bound by customary international law. But the President can also have an enhanced power under international law. For example, under the Geneva Conventions, Article 5 of Convention IV allows a state to detain certain persons as national security threats without trial, although there should be periodic review of that detention.⁶ And the

* Elena Duarte is the Chief of the Cyber and Intellectual Property Crimes section of the United States Attorney's Office in Los Angeles. Ms. Duarte specializes in high technology crimes such as computer intrusion, criminal copyright, criminal trademark violations, trade secrets violations, and Internet fraud. She has been with the Cyber section since it was created in September 2001. As Ms. Duarte stated during her talk, "[a]nything I say or do or give an opinion on during the course of this presentation back to the beginning is my opinion, not the official opinion of the Department of Justice or any component thereof. Thank you."

5. See, e.g., Jordan J. Paust, *Executive Plans and Authorizations to Violate International Law Concerning Treatment and Interrogation of Detainees*, 43 COLUMBIA J. TRANSNAT'L L. 811, 856-61 (2005).

6. Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1948, 6 I.L.M. 318 (1948), 8 U.S.T. 2498 (1948), 118 Consol. T.S. 33 (1948).

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

President is the one that executes international law on behalf of the United States, subject to relevant judicial review.⁷

I see these complexities as part of our domestic legal process, even though the fact context is really transnational if we have foreign Al-Qaeda types here as well. But I would use international law, as our courts have often done, although that does not determine the answer. Furthermore, I would use international law to interpret federal statutes and to interpret constitutional provisions. This makes some of these choices in the choice point areas more complex.

Question from Audience: Al-Qaeda seems to communicate by unusual means, which is why they are so hard to trace. But there are websites through which Al-Qaeda gets their message out and we know that the government is monitoring specific websites that put out information and that are related to Al-Qaeda. Would you say that it is okay to try to disrupt those websites so Al-Qaeda will have a more difficult time communicating? Although it is kind of an endless process, since Al-Qaeda could just generate new websites, it would make their lives harder.

Jordan Paust: Even though this would be happening in our country, the actions that may be taken partly depend on the location of the website. Since use of a website set up elsewhere could involve messages that still come into our country, we potentially could disrupt the information coming in. Our First Amendment applies as the message enters our country, even though it is foreign initiated. The interesting question about cyber-use is where is the use and where is the website actually located.

When we have international networks where there are various states involved, I would assume that our First Amendment applies at least to conduct and messages in the U.S. But the First Amendment does not provide an absolute right of speech, and we are talking about anti-terrorism disruption, perhaps imminent lawless violence.

When you search a website, where is your search? If you initiate the search through your computer system in Maryland, the net could also be going through Canada and Great Britain and into France. Where is the search? And where does the Fourth Amendment apply?

Elena Duarte: If we have an extradition treaty, we can possibly end up charging a foreign target and bringing them back to the United States. The reality is we need two things to catch people: evidence and targets. If the evidence is not here

12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287, available at <http://www.genevaconventions.org>.

7. See, e.g., Jordan J. Paust, *Judicial Power to Determine the Status and Rights of Persons Detained Without Trial*, 44 HARV. INT'L L.J. 503 (2003).

in the United States, ninety-five percent of one's ability to gather it is lost.

When a computer has been hacked into and a trade secret has been stolen, and the hack is traced from a server in the Netherlands, the Fourth Amendment ability to go out and get a search warrant for the content of that website or email address and serve the warrant no longer applies. Unless there is a mutual legal assistance treaty or a Mutual Legal Assistance Treaty (MLAT) process, one cannot even get evidence from another country. Even if there is an MLAT process, there is no uniform requirement of data preservation even in the United States of these Internet service providers and websites.

So if it takes three months to get an MLAT from the Netherlands and in two weeks the Internet service provider in the Netherlands destroys the data, there goes the evidence. Even if someone wanted to go after a perpetrator who has been traced to an IP address in the Netherlands, there is no longer any evidence.

The Fourth Amendment hypothetical is a very good question and it is definitely worth a lot of discussion. But the cold, hard reality of now is that the Fourth Amendment does not cover people in this area. As a matter of fact, limits on getting electronic evidence are actually much stricter than limits on getting ordinary evidence. Someone can go out tomorrow and get your bank records with a grand jury subpoena. But they cannot get your email. Electronic records, like electronic communications, are actually more strictly protected under the law, even here in the United States.

Jordan Paust: When dealing with the location of cybercrime, four different types of states have been identified. First, the state of origin. This is simple, but interesting to think about. For example, the state of origin from which the email bank fraud was attempted, e.g., asking for bank account numbers, might have originated in Nigeria. States of origin would have territorial jurisdiction under international law. With respect to international crimes, states would also have universal jurisdiction if the crime was a customary based international crime.

Second, there are transfer states, but issues concerning transfer states can be complex. Issues include those related to jurisdiction where the cyber-use flows through the state's land territory, air space, or satellites. Cyber space is somewhere and it can be everywhere, so you have the transnational/international net, and in our hypothetical, if we have two transfer states, Great Britain and Canada, do they have jurisdiction over a fraud that began in France? From an international law perspective, yes, they do have jurisdiction. If there is some kind of physical movement of this information through a server located in Canada or a net partly within Canada, Canada has territorial jurisdiction.

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

*Alan Kindred, Moderator*⁸: It is just like a real property law that states that if a plane flies over your land the plane is trespassing without your permission.

Jordan Paust: In addition, there are two other kinds of states: the target state and the storage state. In my hypothetical in which someone located in France is trying to defraud people in the United States, the target state would be the United States.

A given transnational event also might include a storage state. If, for example, the United States was trying to regulate child pornography, the issue of safe haven and storage states might arise. For example, Indonesia might store some of the data and not want to regulate such storage. Even if the United States wants to regulate child pornography and some other states with prescriptive jurisdictional competence also want to have this regulated, these states would have to have an international agreement with Indonesia to require regulation in Indonesia.

We should think about storage and safe haven states and how we should regulate them. The 2001 European Convention on Cybercrime shows that Europe is starting to pay attention to some types of mutual legal assistance enforcement and consent in advance by treaty to some forms of transnational enforcement.⁹ In a limited sense there is some consent in advance for unilateral extraterritorial enforcement, but a lot of the enforcement is still territorial (i.e., to occur within a territorial state only with special consent).

Another question concerns jurisdiction. I mentioned territorial jurisdiction which exists in the state through which information flows. As a substitute for intent, the perpetrator can foresee that the Internet is international in nature and might very well flow through Canada and Great Britain. Therefore, the intent element is met for Canada and Great Britain. Only two out of three elements are required (an act, intent, and effect) to give Canada or Great Britain objective territorial jurisdiction.¹⁰

The innocent agent fiction or agency fiction is also an issue. For example, if I send a letter bomb from Houston into Canada and I am using the mail, the innocent agents helping me perpetrate the crime are acting for me as if by fiction I have acted in Canada, even though they do not know they are helping. This satisfaction of the act element is well recognized under international law. We also have a

8. Alan Kindred is an international intellectual property attorney from Southern California.

9. Council of Europe Convention on Cybercrime, CETS No: 185, Nov. 23, 2001, *available at* <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm> [hereinafter *Convention on Cybercrime*].

10. *See generally* JORDAN J. PAUST, *INTERNATIONAL LAW AS LAW OF THE UNITED STATES*, 417-19 (2 ed. 2003).

continuing act fiction. If I sent a letter bomb through the mail, it is like a bullet that I fired across the boundary and, by fiction, my conduct continues into Canada. The bomb has its injurious effect in Canada, which gives Canada objective territorial jurisdiction (since there is an intent to produce the effect, the effect, and an act in Canada by fiction).

A state will also have nationality jurisdiction, which applies for the state of nationality of the perpetrator. Protective jurisdiction also applies if there are significant national security interests at stake, especially in terms of cyberterrorism. Protective jurisdiction could also be present over other acts that are occurring abroad if the acts otherwise trigger significant national security interests that are directly involved. Universal jurisdiction would apply in cases of crimes under customary international law, such as terrorism. For example, a computer system could be used to facilitate aircraft sabotage, which we recognize as a crime under customary international law implicating universal jurisdiction. These are forms of prescriptive jurisdiction allowing states to enact laws attempting to regulate relevant conduct.

Whether enforcement jurisdiction exists is the critical question, and we have some general principles in international law recognized in the Restatement (Third) of the Foreign Relations Law of the United States, sections 432 and 433.¹¹ The Restatement requires a state to have foreign state consent before enforcing a law in the foreign state's territory. A state can get consent ad hoc from the highest-level officials in a country. For example, in the case of international drug trafficking, a state might get consent of the foreign flag vessel captain because, under the Law of the Sea Convention, he is an appropriate person to give consent on behalf of the flag.¹² Or if a state has immediate telecommunication consent from that foreign flag's state to stop and search that vessel, the state might then get additional consent to arrest and bring the drug traffickers into its own country. The new Cybercrime treaty provides for some consent ad hoc or consent in advance by treaty. It is rare to have certain forms of consent under customary international law and I do not see those forms implicated in this case.

I do see another issue coming up in terms of self-defense. When a state is targeting an Al-Qaeda computer system or network in a foreign state (like Pakistan) that is being used by Al-Qaeda, the state's acts are a permissible measure of self-defense, since there is an ongoing process of armed attack by non-state Al-

11. Restatement (Third) of Foreign Relations Law of the United States §§432, 433 (1987).

12. United Nations Convention on the Law of the Sea, Dec. 10, 1982, available at http://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm.

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

Qaeda actors. This is not law enforcement, it is self-defense. The Security Council may authorize use of military force as well through the U.N. Charter. Some types of interference with other persons' networks could be authorized as part of that package, or by regional organization authorized use of force (e.g., by NATO).

Mutual legal assistance is an important aspect of enforcement. The United States has not ratified the Convention on Cybercrime yet. But on November 9th, 2005, the Senate Foreign Relations Committee gave its consent for a Senate approval and on August 3rd, 2006, the full Senate gave advice and consent to ratification by the President. The executive is obviously thinking about some reservations to this treaty, maybe to protect First Amendment interests, maybe to protect Fourth Amendment interests, whatever the protections mean in this context.

In the future, the United States will likely ratify the cybercrime treaty. And if enough countries have ratified the treaty, it will be operative among those treaty signatories and will be binding on the treaty signatories and their nationals. This treaty looks a lot like a newer type of international criminal law treaty, but a lot of the crimes that states have agreed to create domestically are merely domestic offenses.

There are provisions that are typical in international criminal law concerning jurisdiction. Here, jurisdiction agreed to in the treaty is really consent in advance by the treaty's signatories to some special types of jurisdiction that do not pertain under customary international law. Jurisdiction that we call universal by treaty or universal by consent isn't really universal, but it is universal among the signatories and their nationals.¹³ In other words, if you have a person who committed a violation that is covered by the treaty in your country and the person is found in your territory, you have a circumstance that has triggered an obligation and a competence, which is universal by consent, to bring them into custody and initiate prosecution or extradition, which is a very common scheme in an international criminal law treaty. This treaty has such provisions for jurisdiction. Regarding chapter three, addressing international cooperation, there are a lot of interesting issues in terms of what this treaty requires and allows the signatories to do.¹⁴

In terms of extradition, from an international law perspective the treaty contains a very typical extradition formula. If you do not have an extradition treaty between the United States and Country X, you may consider this to be your extradition treaty vis-à-vis these types of offenses. If you have an extradition treaty, this treaty

13. See, e.g., PAUST, *supra* note 10, at 423.

14. Convention on Cybercrime, *supra* note 9, at ch. 3.

modifies the crimes that are extraditable in a bilateral treaty between the United States and Country X.

There is a dual criminality and duality of sanctions provision that is interesting. The article applies when extradition between parties with respect to the criminal offense is covered, provided that the crimes are punishable by the laws of both parties. This is a customary precept that will be read into any extradition treaty called dual criminality.¹⁵ I also call it duality of sanctions, because, under the treaty, an offense must be punishable by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. So there are limitations in terms of extraditability.

We also have a very typical clause that, some people do not realize, incorporates by reference some forms of domestic preclusions of extradition. For example, the political offense exception can apply under Article 24 Paragraph 5¹⁶ which states that extradition shall be subject to the conditions provided for by the law of the requested party or by applicable extradition treaties including the grounds on which the requested party may refuse extradition. Such a phrase, because it is very typical in the new international criminal law treaties, is really consent in advance to the use of another state's domestic law that might preclude extradition. Some states will not extradite their nationals for these kinds of offenses, which the United States will agree to by ratifying the treaty with respect to offenses covered by the treaty.

I found it curious in terms of international crimes that the United States agreed to this in other treaties. For example, treaties addressing aircraft hijacking, aircraft sabotage, hostage taking, and attacks on internationally protected persons have the same limitations on extraditability.¹⁷ If you cannot extradite, the alternative duty is to initiate prosecution. The United States considers the political offense exception to be a very important customary precept that we will read into extradition treaties. The political offense exception is possibly incorporated by reference in this treaty under Article 24 Paragraph 5. It may not be in the interest of justice, or the Justice Department, to have such a limitation on extraditability but it appears to be part of the treaty package.

There are two types of political offenses. A pure political offense, like espionage, is merely a crime against the state. United States foreign policy prefers to not have people extradited for espionage. But there are relative political

15. *See, e.g.*, ICL, *supra* note 1, at 348, 351.

16. *Id.* at ch. 3, art. 24.

17. *See, e.g.*, ICL, *supra* note 1, at 352.

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

offenses involving instances such as the killing of a human being for a political purpose, and this is where the tension lies and it becomes more difficult to determine whether or not the political exception to extradition should apply. Our courts and our circuits and foreign courts are split in terms of what the test for the exception involves.¹⁸

Elena Duarte: In practice, even if a state has an extradition treaty with a country and after that state has charged someone with a crime and the state extradites that person, it is typically discretionary. Sometimes the state will not extradite at all. There are certain thresholds.

Extradition is a very long, expensive, time consuming process and the United States routinely receives requests to extradite. For instance, when another country apprehends someone that the United States has charged earlier, the country may request extradition. However, unless the crime is of a certain nature or at a certain threshold, the United States will not comply with the request.

For serious cybercrimes, the United States would probably extradite. But for a lot of the lesser crimes, even felonies, extradition is not a very practical remedy.

I can only talk about things that are public record, namely, I will discuss the Zotob worm, from last year. They ended up catching those responsible for the Zotob worm and successfully prosecuting them in Turkey. The Zotob worm cost a lot of people in Los Angeles and the Caterpillar Company a lot of money.

One of the things that we can do, and we need a court order to do it, if an investigation has been ongoing here and we have certain materials that we've gathered with the grand jury and if we decline to prosecute federally, we can release those materials to the state. Otherwise, the grand jury materials are secret within a set of rules — for instance, if the District Attorney's Office is going to prosecute someone that is not prosecuted federally. We can also, with a court order, release the information to foreign governments. If we get a call from China, who doesn't extradite, and they say they've caught an individual. They then ask: What do you want us to do? Do you want to give us what you have and we will look at prosecuting him? The answer to that is generally sure. Then we get a court order because we know if we charge him here we can't get him back. So it is preferable at least to give the other country the chance to prosecute.

Much of what we do is try our best to get evidence. When we cannot get the evidence we need, we get court orders or get permission to try to give out evidence. And the same with people, either we try to get people back or if we

18. See, e.g., *id.* at 348-49, 351, 371-90.
442

cannot get them or the evidence to figure out who they are, at least we can give what we have to the other country.

The example of the e-mail that has traveled through Canada as well as Great Britain is representative of the difficulties of obtaining evidence from different countries. Canada will routinely send back supplemental MLAT requests asking for more information after the initial requests have been made.

Jordan Paust: Getting back to the Council of Europe Convention on Cybercrime, this treaty also has an article for conditions and safeguards with express attention to the European Convention on Human Rights¹⁹ and the International Covenant on Civil and Political Rights,²⁰ which also might raise some issues concerning what is privacy. Much of the powers or authorizations that are based in this treaty are conditioned by human rights law as well.

Europeans have a different view of privacy than Americans, as we know in terms of privacy interests of air travelers. They are unwilling to allow us to have certain information that we would like to have in terms of profiling. So I think it will be interesting to see how Article 15 plays out in terms of human rights safeguards and the European Convention — their interpretation and our interpretation. Who should interpret the European Convention on Human Rights in connection with the Cybercrime Treaty?

Question from the Audience: It seems that there is a frustration with the lack of harmonization in some of those almost more substantive areas. In the European Union there are efforts of harmonization in these various kinds of civil and criminal regulatory regimes. Is that type of harmonization in North America something that would be desirable? Would that facilitate what you're doing?

Alan Kindred: I think it should.

Elena Duarte: Where does it end, though? Because, the reality is that more frequently, in almost every case now and almost every way we have a breach of neutrality. For example, I just finished a trial that was a peer-to-peer case that involved child pornography.

It was on a peer-to-peer file sharing network, and we explained to the jury how peer-to-peer file sharing works. We also had a suppression hearing in front of the judge on how when you look into someone's shared folder on their computer it is not a warrantless search, but it can be likened to one.

19. European Convention on Human Rights, Mar. 20, 1952, 213 U.N.T.S. 262, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>.

20. International Covenant on Civil and Political Rights, Dec. 16, 1966, 6 I.L.M. 368, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

5 SANTA CLARA JOURNAL OF INTERNATIONAL LAW 2 (2007)

Looking into someone's shared folder can be analogized to somebody cutting cocaine on their dining room table with their windows open. Thus, an individual who is walking on the sidewalk, a public place, can see the cocaine. Therefore it is not an illegal search because the individual saw something that was made available for the public to see.

The same thing goes for the analogy of the peer-to-peer file sharing networks. I go out there and I put in my browser I want to look for "kiddie," and it coughs me back up a whole bunch of file titles from share folders that the sharing has enabled and they are there.

So much has happened in the last twenty years and in every case, in every way, every year, things gets more global. In reality we are so far behind what we need to be able to do, I think, and probably most countries are in the same position. In order to work together globally to stop things that most of us probably think should not be going on.

In terms of tools, like the MLATs and the treaties and the things that everybody is trying to do to get us all to work together, even those have so far fallen short of what we really need to use them to do, which is get records in a week and not in a year. Also, the MLATs have to be translated under the treaty even if it is a country where it is pretty obvious that they probably speak English. All the documents still have to be translated and that could take months.

With cybercrimes, the records are fleeting, and there's no international regulation that talks about how long these records need to be kept. Even by the major service providers.