CSCI 1800 Cybersecurity and International Relations

COE Convention on Cybercrime

John E. Savage

Brown University
Outline

• Background
• Provisions of the Convention
  – Cybercrime Offenses
  – Investigative Procedures
  – International Cooperation
• Reaction to and Evaluation of the Convention
• Alternatives to the Convention
What is the Cybercrime Convention?

- First international treaty to address cyber crime.
- It harmonizes national laws on cybercrime and improves national capabilities to investigate such crime. It also increases cooperation.
- Drafted by Council of Europe in Strasbourg in ’01
- US, as experienced observer, played major role.
Origins of Convention

• In 1996 European Committee on Crime Problems (CDPC) set up expert committee on cybercrime.

• They recognized

  – Trans-border nature of such crime,
  – Conflict with territoriality of national laws, & need for concerted international effort to deal with it

• Committee of Experts on Crime in Cyber-space created in February 1997.
Committee Charge

• The Committee of Experts was charged to draft a binding legal instrument addressing:
  – Cyber-space offenses such as illegal funds transfer, services, violation of copyrights and human dignity, protection of minors, offering illegal services.
  – Other substantive crimes involving cyber-space, requiring international cooperation (thus, not cybercrime)
Committee Charge

• The Committee of Experts was charged to draft a binding legal instrument addressing:
  – Use and applicability of coercive powers, such as interception of data, surveillance, search & seizure of data, problems caused by encryption, etc.
  – Questions of jurisdiction on cyberspace offenses, e.g. double jeopardy, which laws apply, etc.
  – International cooperation investigating cyberspace offenses
Emergence of Convention

- After four years of work, in June 2001 final draft of the convention was approved by CDPC.
- Adopted by Council of Europe on Nov. 8, 2001.
- Convention entered into force in US on Nov 1, 2007
- Convention open to all COE member states.
  - As of 4/25/2016 48 states have ratified, 6 others signed.
- States may be invited to accede to it after obtaining consent of “contracting states.”
Additional Protocol

• Adopted by Committee of Ministers on 11/7/02
• Requires states to criminalize
  – Racist or xenophobic acts, threats, etc via networks
  – Denial of the Holocaust and other genocides.
  – These all involve criminalizing content!
• US helped draft this protocol but did not sign it
Provisions of the Convention

• Goals:
  – Protection of society from cybercrime
  – Criminalization of such conduct
  – Adoption of powers sufficient to combat above
  – Help other states with crime detection, investigation, prosecution
  – Provide for fast reliable international cooperation
    • Mutual Legal Assistance Treaties (MLATs), the alternative vehicle for this, is very slow.
Convention Has Three Parts

1. Listing of substantive cybercrime offenses that ratifying states must adopt into national law.
2. Investigative procedures that states must implement.
3. Mechanisms to enhance international cooperation.
Convention Requirements

• Ratifying states must create laws allowing:
  – Search and seizure of computers and data
  – Wiretapping
  – Obtain real-time and stored communications data
  – This applies even if crime not considered a “cybercrime”

• Thus, Cybercrime Convention is a misnomer.
Definition of Criminal Offenses

• Access to computer systems without right.*
• Technical interception of non-public data to from or within computer systems without right.
  – Includes electromagnetic emissions from computer
  – Does it include audio recording of key strokes?
• “Damaging, deleting, deteriorating, alteration or suppressing of computer data without right.”
• Serious hindering of “functioning of computer system by inputting, transmitting, deleting, deteriorating or suppressing of computer data.”

* The 1986 Computer Fraud and Abuse Act (CFAA) applies to this issue.
Criminal Offenses

- “Production, sale, procurement for use, import, distribution” or possession of “a device, including computer program, designed or adapted primarily for the purpose of committing any of the [above].”
- The same applies to a “password, access code, or similar data” used to access a computer system.
- “Causing of a loss of property to another” by actions of above type with the intention personal benefit when done without right.
Criminal Offenses

- Production, distribution, offering, procurement or possession of child pornography via computer done without right.
- Willful infringement of copyright and related material when done “on a commercial scale and by means of a computer system.”
- All parties must ensure that listed offenses “are punishable by effective, proportionate and dissuasive sanctions including deprivation of liberty.”
What Crimes Are Missing?

• Is IP hijacking a crime (BGP)?
• How about DNS fraud (violating trust in DNS)?
Investigative Procedures

• Parties must establish following legislate powers:
  – Power to order preservation of computer data and traffic data (identifies path of packets thru ISPs).
  – Power to seize computers and storage media
  – Power to order production of computer data and subscriber information.
  – Power to collect such traffic data in real time.
  – For serious crimes, power to collect content in real time.
  – Establish jurisdiction over substantive offenses in Convention committed at home or against another.
International Cooperation

• All Parties “shall co-operate with each other … to the widest extent possible” on these matters.
• Cooperation is thru relevant international agreements and domestic laws.
  – Thus, cooperation may be limited or delayed
• Offenses punishable domestically by year in jail or more severe must be seen as extraditable.
  – However, limits to extradition may come into play.
International Cooperation

• To extent permitted under domestic law, Parties must forward info it believes may help other Parties to investigate cybercrime.
  – Parties may request such info be kept confidential

• When Parties don’t have mutual legal assistance treaty or arrangement, each must designate a central authority to send, answer, request mutual assistance.
  – Parties agree to execute requests in accordance with procs. of requesting Party, except where incompatible
International Cooperation

• Parties must preserve data expeditiously and for at least 60 days at request of another.
  – A Party may refuse a request for variety of reasons.

• Party must respond to a request to search, seize or disclose data located within its territory.
International Cooperation

- Parties must provide mutual assistance in the real-time collection or recording of content data ... to the extent permitted under laws and treaties.
- Each Party must have a person on call 24/7 to respond to assistance requests in investigations.
- Convention lacks enforcement mechanism. Instead CPDC is informed of interpretations/applications.
  - Arbitration is possible for disputes concerning the latter.
International Cooperation

• Party may access “without authorization of another Party” data on computer in territory of the other if lawful and voluntary consent obtained from person with authority to provide it.

  – Russia signed the convention but withdrew when it realized implications of this provision.
  – If they were to rejoin, other nations would as well!
Competition for the Convention

• International Telecommunications Union (ITU), a UN agency concerned with ICT issues, challenged universal adoption of Convention, circa 2010.
• ITU General Secretary Hamadoun Torré objects because it is Euro-centric and “a little dusty.”
• ITU has “ITU Toolkit for Cybercrime Legislation” drafted by American Bar Association committee.
• ITU promoted its own cyber-warning org., IMPACT.
Evaluation of Convention

- “Most substantive, and broadly subscribed, multilateral agreement on cybercrime” today.
- Relatively comprehensive approach to harmonizing national laws and cooperation.
- US DoJ official rates impact: “very positive.” Cooperation has increased radically recently.
- Provisions to freeze data, “spontaneous” cooperation, 24/7 contact, remote searches are most useful.
Evaluation of Convention

• Shortcomings:
  – Russia and China not signatories. No states from Africa or South America.
  – Parties may refuse to assist in many instances
  – No enforcement mechanisms
Evaluation of Convention

• Shortcomings:
  – Does not address espionage or use of force under laws of war
  – Does not deal with issues that arise when a nation is under attack and can’t afford to wait for cooperation from countries that may be attacking.
  – Doesn’t apply to DNS fraud or IP hijacking (BGP).
Possible Steps for Improvement

• Narrow grounds for rejecting request for assistance
  – Require specific reasons for denying requests in writing

• Add meaningful enforcement mechanism
  – Require neutral arbiter when request denied

• Require reporting of denials of assistance to CDPC

• Authorize those Parties denied assistance without legitimate, credible reason to engage in unilateral, cross-border investigations.
  – Would this violate sovereignty?
Alternatives to the Convention

• Most notable is Russian cyber arms treaty
  – In ‘98 it equated cyber weapons with weapons of mass destruction
• In 2000 Russia sponsored UN General Assembly resolution to examine ways to strengthen “security of global information and telecommunications systems” and “limit threats emerging in this field.”
2000 Russian Proposal

• States must refrain
  – “from development, creation, and use of means of influencing or damaging another State’s information resources and systems,”
  – “deliberate use of information to influence another State’s vital Structures,”
  – “unauthorized interference in information and telecommunications system and information resources, as well as their unlawful use,”
  – “encouraging the activities of international terrorist, extremist or criminal associations, organizations, groups or individual law breakers that pose a threat to the information resources and vital structures of States.”
2000 Russian Proposal

• How does one interpret “influence”? 
• What is “unauthorized interference”? 
• What are “international terrorist, extremist or criminal associations, organizations, groups” and “vital structures of States”?

• Are the Russians more concerned about “state security”?
Recent Russian Proposal

• In 2008 Vladislav Sherstyuk, deputy secretary of the Russian Security Council, proposed a treaty that would prohibit secretly embedding malicious code in a country’s computers for later use in event of hostilities.

  – Note: US DoD now considering this!

• Russia also proposed prohibiting attacks on non-combatant systems as well as deception in cyberspace.
US Response to Russian Proposals

• US has been to cool to these proposals.
• US started meeting with Russians in late 2009 and agreed to talk at UN Disarmament & International Security Committee.
• 4/10 US attended Garmisch cybersecurity conf.¹
• Gen. Keith Alexander, head of Cyber command, said “what Russia put forward is, perhaps, the starting point for international debate.”

¹ Fourth International Forum Partnership of State Authorities, Civil Society and the Business Community in Ensuring Information Security and Combating Terrorism, Garmisch-Partenkirchen, Munich, Germany.
Alternatives

• Gen. Alexander: US should develop counter-proposal to Russia’s proposed treaty.
• Russian proposals did not gain traction initially.
• Seems unlikely that US would agree to ban offensive cyber weapons soon.
• In ‘15 the UN GGE and G20 adopted this norm:
  – No country should intentionally damage the critical infrastructure of another.
  – It was originally a Russian proposal.
Review

• Background
• Conventions Provisions
  – Cybercrime Offenses
  – Investigative Procedures
  – International Cooperation
• Reaction to and Evaluation of the Convention
• Alternatives to the Convention