CYBER POLITICS AND POLICIES

CHAPTER 7: CYBERCRIME

AT THE END OF THIS CHAPTER, STUDENTS WILL BE ABLE TO:

- Describe major types of cybercrimes, distinguishing between high and low policing and cybercrime vs. cyber-facilitated crime
- Describe attempts to combat cybercrime, including legislation, on the state and international levels
- Formulate a position on the ethical, social and legal issues related to preemptive policing and surveillance

DOES THE INTERNET FACILITATE OR ENCOURAGE CRIME?

TECHNOLOGY ATTRIBUTES

- Attribution problem
- Dark Web
- Anonymity
- Transnational internet
- Peer to peer networking

SOCIAL/POLITICAL ATTRIBUTES

- Jurisdiction problems
- Difficulties in coordinating an international response to cybercrimes
- TRUST/FRAUD issues: relationship fraud, bank fraud, identity theft
- Radicalization and polarization

DEFINING CYBER CRIME

- **Computer-enhanced crimes / computer-facilitated crimes:** Existing crimes (like identity theft) which are now being carried out in the online environment.
- **Computer crimes:** fundamentally new. Sending malware, viruses, DDos attacks, worms, cyber vandalism.

TYPES OF CYBER CRIMINALS

- Hacktivists
- White Hat Hackers
- Black Hat Hackers
- State-sponsored cyber criminals
- Cyber terrorists

HIGH CRIMES VS. LOW CRIMES

High crime/Tier 1 Threat: affecting a state's national security (can include cyber terrorism, threats to critical infrastructure)

- Advanced Persistent Threat
- cyber-espionage carried out by states aimed at stealing commercial or military technologies of other states;
- PSYOPS aimed at undermining a state's reputation and relationships with voters and citizens.
- The United States Criminal Code Provision 18 of the USCS section 1030(a) (a) has the most stringent criminal penalties for those accused of seeking or achieving unauthorized access to government computers. Accessing government computers can carry a sentence of up to 10 years in prison with longer sentences for repeat offenders.

Low crime – not against state; not significant to national security

THE ROLE OF THE STATE IN COMBATTING CYBERCRIME

Computer Fraud and Abuse Act (CFAA)

most comprehensive set of statutes regarding the criminal use of computers, covering everything from hobby or nuisance hacking up to and including espionage and state-sponsored hacking.

The CFAA also covers such criminal enterprises as the trafficking in passwords, or the theft of trade secrets.

CFAA has also been used creatively to charge individuals who have engaged in cyberbullying and cyberstalking through the creation of fake websites and identities online.

- Jurisdiction Issues: US versus Microsoft, 2014
- Mutual Legal Assistance Treaties (MLAT)
- Sovereignty Issues

PUBLIC PRIVATE COOPERATION IN COMBATTING CYBERCRIME

- **Online Trust Alliance (OTA)**
- **Industry Botnet Group (IBG).**
- **National Cyber-Forensics and Training Alliance (NCFTA)**

- US

- **Government Computer Emergency Readiness Teams (CERTs)**
- **Cyber Threat Intelligence Program (C-TIP)**

ATTEMPTS TO CREATE INTERNATIONAL FRAMEWORKS TO COMBAT CYBERCRIME

- Budapest Convention on Cybercrime
- Arab Convention on Combatting Information Technology Offenses
- Common Market for Eastern and Southern Africa Cybersecurity Draft Model Bill

CYBER OPTIMISTS VS. CYBER PESSIMISTS: COMBATTING CYBERCRIME

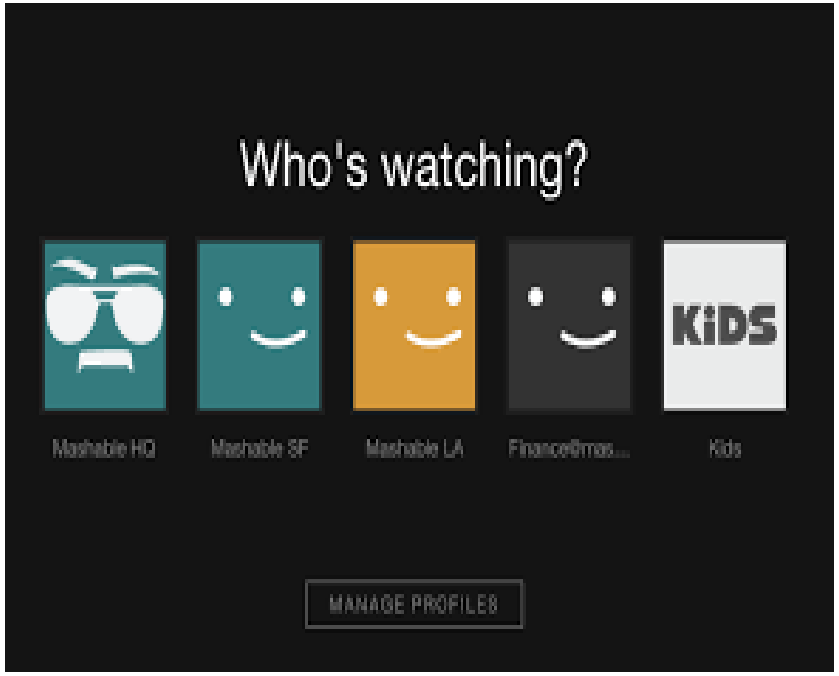
- Dependence of states on actors like public-private cooperation, international coordination – is proof that states cannot handle the threat of cyber crime on their own.
- It is a sign of weakness

- *The ability to states to engage in cooperation with a variety of actors – including private corporations and other nations – to combat cybercrime, shows that states have the flexibility and creativity to succeed in overcoming this threat.*

CRIME AS A SOCIAL CONSTRUCT

Cultural Factors: Which of these do you consider to be CRIMINAL BEHAVIOR?

1. Borrowing a Netflix password
2. Engaging in homosexual activity
3. Going out in public without a head scarf
4. Searching for information online about how to impeach a president or other ruler



DEFINING INTELLECTUAL PROPERTY

- "Creations of the mind, such as inventions, literary and artistic works, designs and symbols, names and images used in commerce"

THE PROBLEM OF HATE SPEECH, ONLINE RACISM, HARASSMENT

- Budapest Convention on Cybercrime currently includes 'additional protocols' which deal with questions of racist and xenophobic (anti-foreigner) speech. The Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic nature Committed through computer systems

- Does policing speech online violate Freedom of Speech?
- Should individuals or groups be banned from the internet? Why or why not?

AN INTERNATIONAL CONVENTION ON TRANSNATIONAL CRIME?

- **2000: United Nations Convention against Transnational Organized Crime (TOC)**
- Offense is transnational
- if was committed in more than one state;
- committed in a single state but planned, prepared, directed or control by another state;
- committed in one state but involved an organized group whose activities cross national boundaries
- committed in a single state but with substantial effects in another state.

2001: The Council of European Cybercrime Convention (or Budapest Convention)

3 aims:

- to lay out common definitions of certain criminal offenses
- to define common types of investigative powers better suited to the information technology environment
- to determine both traditional and new types of international cooperation.
- Title Three: defined content related offenses – including using computers as a vehicle for sexual exploitation and acts of racist or xenophobic nature.
- Title 4 defined offenses related to intellectual property and copyright.

CYBER OPTIMISTS VERSUS CYBER PESSIMISTS

- "There is now a positive 'moral climate' for enforcement action, whether by civil, criminal or administrative measures and this cross-border cooperation recognizes what sociologists call 'communities of shared fate.

- Cyber pessimists point to the weaknesses of existing vehicles like the Budapest Convention. They argue that the Budapest Convention is largely symbolic with few 'teeth' to really enforce the treaty's provisions. The convention seeks to harmonize existing international legislation but many signatory states do not actually have strong and binding domestic laws regarding the investigation and prosecution of cybercrime.

CYBER CRIME IS NOT A STAND-ALONE ISSUE

- issues are frequently entangled with issues of national security, economic competitiveness, and national power in the international system.
- impossible to speak about steps the US is taking to combat and counter Chinese cyber-espionage, including the theft of US trade secrets, without taking into account the larger US-China relationship, including the ways in which the US and China are competing for economic power and political influence in the global economy.

THE ISSUE OF SURVEILLANCE/ANTICIPATORY POLICING

- Profiling
- Relation to due process/ "potentially guilty in the future" is not the same as 'innocent until proven guilty'
- DIFFERENTIAL SURVEILLANCE

- Use of algorithms to predict which individuals and GROUPS of people are likely to be criminals

FOR DISCUSSION

- Do you believe that individuals behave differently in cyberspace than they do in real life? In what ways? What, if anything, can be done to cause people to behave in a socially responsible way in cyberspace?