Cybersecurity & International Law

Matthew C. Waxman
Liviu Librescu Professor of Law
Columbia Law School
Outline

• Some International Law Basics
• Cyber-Attacks and Cyber-Warfare
• Cyber-Espionage
• Cyber-Crime
• Other Issues
• General Take-Aways
Some Basics

• 2 basic types of international law:
  
a) “Treaty Law”: formal agreements among states to be legally bound
  
b) “Customary International Law”: general & consistent practice followed out of a sense of obligation
  
• Change in international law is generally slow…
  … but technology is changing fast
Cyber-Attacks and Cyber-Warfare (I)

- There is a well-established body of int’l law regulating armed response to physical/kinetic military attacks against states.
- There is also a well established body of law regulating kinetic military attacks once conflict is underway.
- To what extent – if any – do those rules apply to cyber-attacks?
  - May a state respond to cyber-attacks with military force?
  - Must cyber-attacks comply with rules of distinction, proportionality, etc.?
Cyber-Attacks and Cyber-Warfare (II)

- Emerging consensus that “normal” rules of physical space apply, but big questions of interpretation

- Some of these differences over framework have been bridged, but major interpretive, technical, and policy questions remain:
  - What types or magnitudes of attacks trigger a right of armed self-defense?
  - Sovereignty? Counter-measures to low-level attacks?
  - What sorts of cyber-attacks violate the laws of war?
  - Attribution: how to deal with uncertainty?

- These questions are difficult to answer in abstract/advance and will remain highly contentious in practice
Cyber-Espionage

• Is espionage legal?
  – No
  – Yes
  – Maybe/sort of

• Is cyber-espionage special?

• Is “industrial” espionage special?
Cyber-Crime

• Budapest Cybercrime Convention (under auspices of Council of Europe)
  – About 40 (mostly western) state parties
  – Obligates state parties to enact laws to be able to prosecute cybercrime internally
  – Calls for mutual assistance in investigating/prosecuting
  – Contains exceptions for protecting state interests
  – Other states are joining, but many major players are not, and still others are developing parallel agreements

• Big challenges to prosecutions (extradition, bilateral legal assistance, etc.)
Other Issues

• Internet governance
• Human rights
• International trade/export controls
• “soft law”, norms, codes of conduct
General Take-Aways

• Why no major cyber-security treaty?

• Expect a patchwork of international legal efforts to deal with specific issues – and there will be major gaps

• International law has limits to effectiveness, but it’s a powerful tool – so states are vying to shape it to their interests

• Many challenges are not as novel as they may seem at first (or as they are often described)
Cybersecurity & Domestic Law

Matthew C. Waxman
Liviu Librescu Professor of Law
Columbia Law School
Outline

• Some General Points
• Protecting Critical Infrastructure
• Countering Hacking
• Surveillance
General Points

• Paces of change

• Complexity: horizontal & vertical allocations of power

• Range of legal tools
  – Authorities and their allocation
  – Direct regulation
  – Liability
Protecting Critical Infrastructure

• Much of it is privately held -- is it adequately protected?

• If not, more regulation?
Countering Hacking

• Criminal law: e.g. Computer Fraud and Abuse Act

• Allocating liability/disclosure requirements

• How to encourage information sharing?

• “Hacking Back”/“Active Defense”
Surveillance

• Intersections of cybersecurity & surveillance

• Complex patchwork of law, e.g.
  – 4th Amendment jurisprudence
  – Wiretapping statute, FISA, ECPA
  – Executive orders and guidelines

• “Going Dark”/Encryption Issues