INTERNATIONAL LAW OF CYBER OPERATIONS
The Lineage

- 1990s: United States Naval War College
- 9/11
- 2004-2017: UN GGE
- 2007-08: Estonia & Georgia
- 2009-12: Tallinn Manual
- 2013-17: Tallinn Manual 2.0
- 2017: This course
What this course is not…

• The policy of any country or organization

• A platform to convince you Tallinn Manual 2.0 has all the right answers
Purpose of This Course

• Help you “issue spot”
• Identify where the law is relatively certain
• Identify where it is unsettled, so you can assess risk
• Help you determine own State’s legal position, policies, rules of engagement
Sources of International Law

• Primary sources
  • Formal agreements
    • Bilateral
    • Multilateral:
      • E.g., Budapest Convention on Cyber Crime
  • Customary practice
    • This course
  • General principles of law
    • Good faith
Sources of International Law

- **Subsidiary sources**
  - Judicial decisions
    - E.g., US Supreme Court’s Microsoft Case
  - Writing of publicists
    - E.g., Tallinn Manual 2.0

- **Careful: Is only the outer limit**
  - Domestic (regional) law and regulation may be more (not less) restrictive
    - General Data Protection Regulation (GDPR)
International Law-Making

• Only **States** create international law
  • Consent based

• **Individuals/groups** do not participate as such directly
  • But...absence of State action, can de facto move law
Treaties

- “[T]reaty...international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation.” VCLT (1969), Art. 2(1)(a)
  - UN Charter
  - Additional Protocol I
  - Budapest Convention
  - SCO Agreement on Cooperation in the Field of International Information Security (Yekaterinburg Agreement), 2009
Treaties

- **Recognise** existing customary norms
  - Genocide Convention

- **Create** new rights and obligations
  - Budapest Convention

- **May allow** otherwise unlawful conduct
  - Example: Basing agreement that allows another State to conduct cyber operations from military base on territory

- **Binding only on** States parties
  - But may “crystallize” into customary law
    - Vienna Convention on Law of Treaties
Reservations:

• **Exclude or modify** legal obligation (if treaty does not exclude)

• **Budapest Convention art. 42**
  
  • By a **written notification** addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, **declare** that it avails itself of the **reservation(s)** provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. **No other reservation may be made.**
Reservations: Example

• Article 4 – Data interference

1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Customary International Law

• “International custom, as evidence of a general practice accepted as law.”

ICJ Statute, Art. 38(1)(b)
Customary International Law

- **State practice**
  - Official government *conduct*
  - Official statements at int’l conferences, UN voting, diplomatic exchanges, formal instructions to diplomatic agents, national court decisions, legislative measures or other actions taken by governments to deal cyber matters
- **Inaction** (Nuclear Weapons Advisory Opinion)
  - Refraining from engaging in cyber ops with physical consequences

- **Widespread**, although not universal
  - Include *specially affected* States
  - May *not be significant number* of States that consistently *reject*
    - Sovereignty in cyberspace?

- **Over time**
Customary International Law

- **Opinio Juris**
  - May 2018 UK Attorney General statement

- Customary law binds all States
  - Even States that did not participate
  - Persistent objector during formative stage:
    - Objection must be express
    - Some scholars reject

- May alter pre-existing norm
  - E.g., State monitoring and the right to privacy
Obstacles: Customary International Law and Cyber

- Lack of State practice
- Classified nature of State practice
- General absence of *opinio juris*
- Widespread in cyber context?
- Over time in cyber context?
International Law of Cyberspace

• Very limited cyber-specific international law, so…

• Pre-cyber international law
  • General international law
    • Examples: Sovereignty and State responsibility
  • Specialised regimes
    • Examples: Law of the sea and international humanitarian law
Soft Law

• Not binding…but often influential

• Examples: guidelines, policy declarations or codes of conduct
  • UN GGE Reports
  • UN General Assembly Resolutions
    • Unless meant to restate customary law
  • SCO Code of Conduct
UN GGEs

• UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)

• Under UN General Assembly’s First Committee
  • Disarmament and International Security

• Five GGEs between 2004 and 2017
UN GGEs

• **2004-2005, 15 nations, no report**
  - Belarus, Brazil, China, France, Germany, India, Jordan, South Korea, Malaysia, Mali, Mexico, Russia, South Africa, United Kingdom, United States of America.

• **2009-2010, 15 nations**
  - Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, South Korea, Qatar, Russia, South Africa, United Kingdom, United States of America.

• **2012-2013, 15 nations**
  - Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, United Kingdom, United States of America

• **2014-2015, 20 nations**
  - Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Republic of Korea, Russia, Spain, United Kingdom, United States of America

• **2016-2017, 25 nations, no report**
  - Australia, Botswana, Brazil, Canada, China, Cuba, Estonia, Finland, France, Germany, India, Indonesia, Israel, Japan, Kazakhstan, Kenya, Mexico, the Netherlands, Republic of Korea, Russia, Serbia, Spain, Switzerland, United Kingdom, United States of America
2016-17 GGE

• 23 June failure to issue report

• China, Russia, Cuba, others reject text on:
  • Right to respond to internationally wrongful acts (a veiled reference to countermeasures)
  • Right to self-defence
  • International humanitarian law

• But…Nov 2018, UNGA 1st Committee
  • US Resolution for new GGE on int’l law and norms
  • Russ. Resolution– Open-ended working group to consider past reports, identify new norms
New and On-Going Initiatives

• 2018 UN General Assembly
  • New GGE
  • Open-Ended Working Group (OEWG)

• Paris Call for Trust and Security in Cyberspace

• Global Commission on the Stability of Cyberspace

• Private sector initiatives
  • Cybersecurity Tech Accord
  • Siemens Charter of Trust
  • Microsoft “Digital Geneva Convention”
Confidence Building Measures (CBMs)

- Cold War & nuclear weapons
- To prevent outbreak of conflict by miscalculation or misperception
- Processes on crisis management cooperation, stability, transparency
- ‘Politically’ binding
- Organisation for Security and Co-operation in Europe (OSCE)
  - Information sharing (policies, critical infrastructure)
  - Contact points, consultations
  - CERT cooperation
OAS Working Group on Cooperation and Confidence-Building Measures in Cyberspace

• Inter-American Committee against Terrorism
  • CICTE Res. 1/17
  • April 2017

• Tasked to “prepare a set of draft … (CBMs), based on the consensus reports of the … UN GGE to enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict
Regional Developments: OAS

• Working Group on Cyber Crime (2016 Meeting)

  • …establish, as soon as possible, specific units or bodies charged with managing and conducting the investigation and prosecution of cybercrimes

  • …adopt or update the legislation and procedural measures that are specifically required to criminalize the different forms of cybercrime and that ensure the efficient, effective, and timely investigation and prosecution of cybercrimes and enable States to cooperate with one another in the investigation and prosecution of those crimes

  • … adopt…legislation to ensure collection and safe custody of all forms of electronic evidence for service providers to guarantee the preservation and recovery of information that is stored or in transit
Regional Developments: OAS

• The Inter-American Integral Strategy to Combat Threats to Cyber Security (2004)
  • Secretariat of the OAS Inter-American Committee against Terrorism
  • Secretariat to help establish CSIRTS
  • Create network of CSIRTS
  • Support development of national cyber security strategies
• Continue efforts to establish, and/or strengthen, national cyber incident alert, watch, and warning groups (CSIRTs)
  • Participation in Secure Hemispheric Network of CSIRTs & other Cyber Security Authorities
  • Increasing information sharing and cooperation

• Enhancing the security and resilience of critical information and communications technology (ICT) infrastructure against cyber threats,
  • Particular focus on critical governmental institutions as well as those sectors critical to national security, including energy, financial, transportation and telecommunications systems

• Intention to continue developing comprehensive national cyber security strategies

• Promoting public sector cooperation with the private sector and academia

• See also, *Inter-American Cooperation Portal on Cyber-Crime:*
QUESTIONS?