CSCI 1800 Cybersecurity and International Relations

Development of Cyber Norms

John E. Savage

Brown University

Outline

- The norms development process
  - Evolution, emergence, framing
- Phases of cyber norms development
  - Contestation, Translation, Emergence, Internationalization
- Role of US (Secretary Kerry) and UN GGE
  - Bilateral agreements
- Microsoft norms
- GCSC and EWI joint norms universalization project
- Charter of Trust
- OEWG vs GGE outcomes

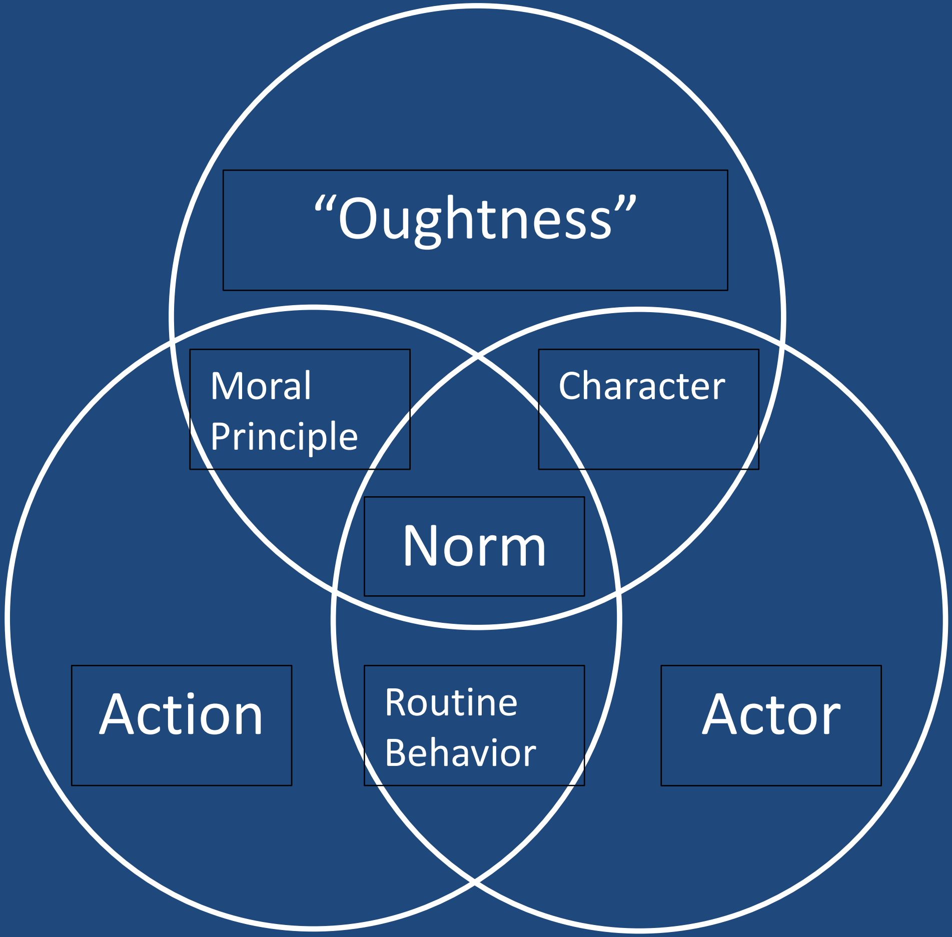
What are Norms?[†]

- Norms are the collective expectations for the proper behavior of actors with a given identity*
  - Must be based on shared beliefs among key players
- How do norms relate to law and principles?
  - Principles articulate goal or vision of group behavior
    - Norms link specific actors to behavior, principles do not
  - "Law is a system of rules … created and enforced through social or governmental institutions to regulate behavior." – Wikipedia

† Martha Finnemore, *A Short Primer on Norms*, http://cybersummit.info/sites/cybersummit.info/files/book2017.pdf

* Peter J. Katzenstein, ed., The *Culture of National Security: Norms and Identity in World Politics.* New York: Columbia UniversityPress, 1996, p5.

What Isn’t a Norm – M. Jurkovich*


“Oughtness”

Moral Principle

Character

Norm

Action

Routine Behavior

Actor

* http://cs.brown.edu/courses/csci1800/sources/2019_IntlStudiesRev_WhatIsntANorm_RedefiningTheConceptualBoundariesOfNormsInTheHumanRightsLiterature.pdf

Norm Evolution

- Norms often start as best practices
  - Experience helps refine them into norms
  - E.g. Lack of “due diligence” leads to liability
- Some norms emerge as law
  - Importance of a norm to society is a factor
- No mechanism exists to enforce international laws
  - E.g. There is no international police force
  - But sanctions can be imposed
- Today cyber norms preferred to international law
  - Because cyber is changing too rapidly

How Norms Emerge

- Some norms emerge spontaneously from habit
  - E.g. Deployment of a protocol by many companies
- Norm reversal may require action
  - E.g. Sanctions to make IP theft unacceptable
  - E.g. US indictment of five Chinese hackers in 2014
- Most norms require hard work
  - Norm entrepreneurs play an important role
  - E.g. H. Dunant, founder of Red Cross
  - Microsoft in ‘14 at EastWest Global Cyberspace Coop. Summit
- Influential actors can help norms emerge
  - E.g. 2015 US/China action on IP theft serves as a model

The Importance of Framing

- Norms promotion is about persuasion
- Thus, framing is important
  - I.e. How we organize, perceive, communicate reality
- Framing is often influenced by events
  - E.g. DDoS attack on Estonia was highly visible
- Small players may be more effective than larger
- Shared beliefs influence framing & they change
  - E.g. Attitudes toward landmines

Do Cyber Norms Matter?

- Chinese theft of US IP for economic benefit declines precipitously
  - FireEye:
    - Number of IP thefts ~65/month in mid 2014
    - By 12/15 it as was < 5/month
    - But, apparently decline was underway by 9/15
  - Crowdstrike:
    - 10/16 - 90% decline in commercial hacking reported
- Progress was due to many years of hard work

Phases of Cyber Norms Development*

- Healey and Maurer identify three phases:
  - – Contestation
    - Existing laws don't apply. Something new needed
  - – Translation
    - How could existing law be translated to cyberspace
  - – Emergence
    - Speech in Seoul by Sec. Kerry in May 2015 significant
  - – Internationalization
    - UN Group of Government Experts (GGE) 7/2015 report

- Healey and Maurer, *What it'll take to forge peace in cyberspace*, Christian Science Monitor, March 20, 2017
- https://carnegieendowment.org/2017/03/20/what-it-ll-take-to-forge-peace-in-cyberspace-pub-68351

Contestation

- 1998 Russian call for cyber arms control treaty
- US response:
  - It sees this as attempt to limit US superiority
  - Skeptical that can negotiate, enforce, verify treaty
  - Prefers existing treaties, e.g. Geneva Convention
  - Proposes five unanimous UNGA resolutions
    - Reason: good defense better than constraining offense

Contestation

- 2011 London Process* – US & UK propose aspirational "Rules of the Road" for govts.
  - The London Process resulted in annual meetings
- 2011 US develops its International Strategy for Cyberspace†
  - After ignoring Russian approach to UNGA First Committee on disarmament, US agrees to the UNGGE process

* https://www.thegfce.com/news/news/2016/12/20/india-host-of-fifth-gccs

† https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

First UN GGE Ends Contestation

- 2013 The UN Group of Governmental Experts, 15-member committee, including China, Russia and US, affirms
  - International law and the UN Charter are applicable online just as they are offline
  - Important because some say new cyber law needed
- Cyber norms now seen as precursor to customary international law
- 2013 marked the end of the contestation phase

Translation

- In parallel, norm translation was underway
- How could existing customary international law and treaties be translated to cyberspace?
  - US, UK, Aus assert LOAC* apply to military cyber ops
  - But, no detail on how LOAC could be interpreted
- Tallinn Manual on International Law Applicable to Cyber Warfare provides first cut at the application of LOAC to cyber

* LOAC is law of armed conflict.

Emergence – Kerry’s 2015 Speech*

Secretary State Kerry’s speech, at Korea University, Seoul, May 18, 2015

1. [T]he basic rules of international law apply in cyberspace.
2. Acts of aggression are not permissible.
3. [C]ountries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.

* https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm

Secretary Kerry’s May 2015 Speech

- We also support a set of additional principles …

4. No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another’s critical infrastructure.
5. No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm

Secretary Kerry’s May 2015 Speech

- We also support a set of additional principles …

6. No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain
7. Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way
8. Every country should do what it can to help states that are victimized by a cyberattack.

Microsoft 2015 Norms*

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

* http://aka.ms/cybernorms

Microsoft 2015 Norms*

4. States should commit to nonproliferation activities related to cyber weapons.
5. States should limit their engagement in cyber offensives operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

* http://aka.ms/cybernorms

Reservations Expressed about Norms

- Harvard Law Professor Jack Goldsmith*
  - Asks why would a nation agree to such norms
  - Wouldn't they act out of self interest?
- But what if they benefit from acceptance?
- As we saw earlier, Kerry norm #6 has led to reduction in IP theft for commercial purposes
  - Could that be due to recognition by Chinese companies that they don't want to lose their IP?

* https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf

Internationalization

- July 2015 the UN GGE* (20 countries) proposes:
  1. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
  2. States, in ensuring the secure use of ICTs, should respect … the promotion, protection and enjoyment of human rights on the Internet…;
  3. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure…;

* http://cs.brown.edu/courses/csci1800/sources/2015_GGE_Norms.pdf

Internationalization

4. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.
5. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
6. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams … of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Next Steps

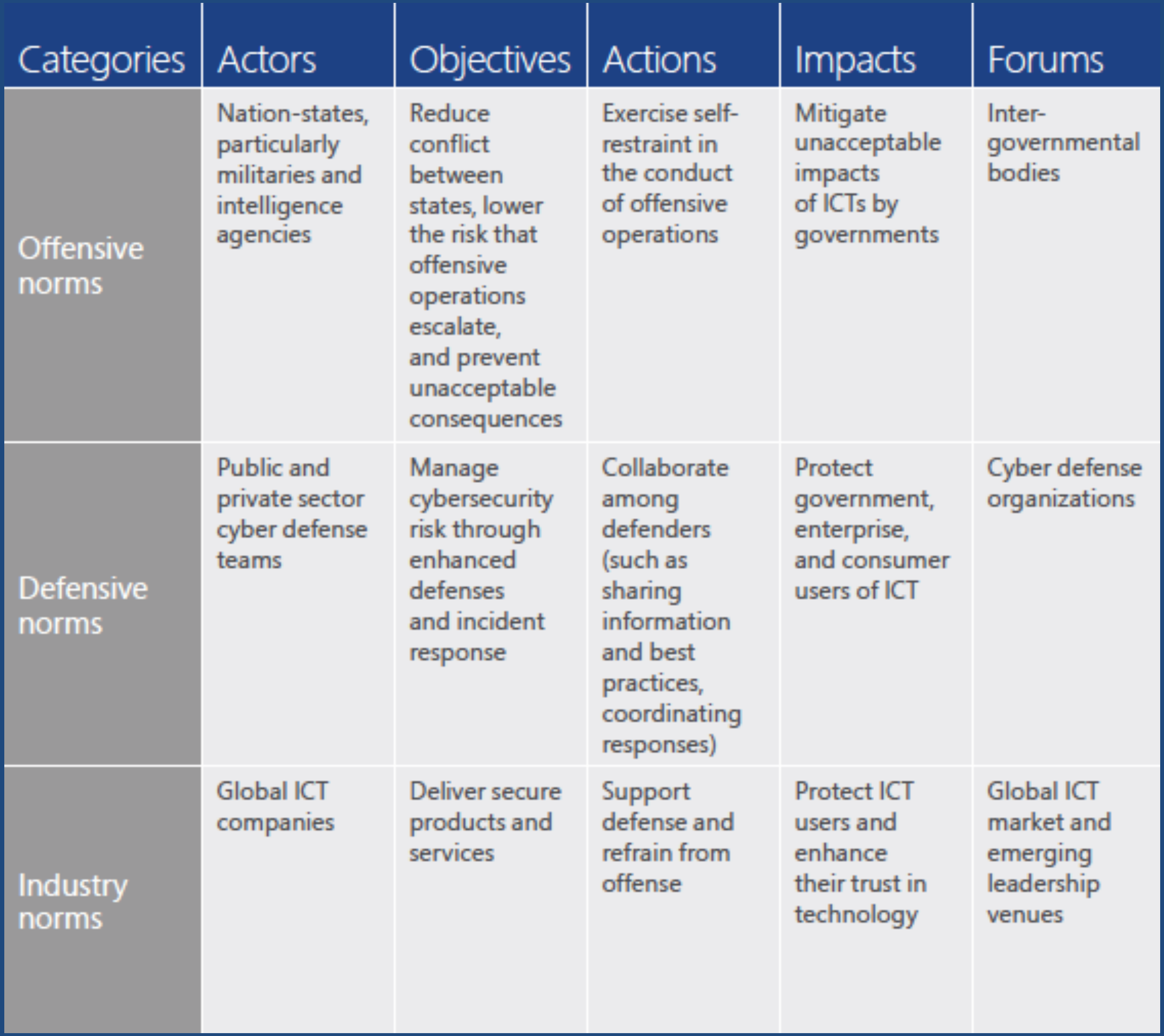
- September 2015 Presidents Xi and Obama:
  - Agree that timely responses should be provided to requests for information and assistance concerning malicious cyberactivities.
  - Agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
  - Similar UK/China & Germany/China bilateral agreements following US/China bilateral
- G20 accept the 2015 UN GGE norms

A Role for the Industrial Sector*

- "[C]yberspace … is produced, operated, managed and secured by the private sector."
- "[T]he targets in this new battle – from submarine cables to datacenters, servers, laptops and smartphones – … are private property owned by civilians."
- "A cyber-attack by one nation-state is met initially not by a response from another nation-state, but by private citizens."
- Microsoft introduces norms in 2014-16. Goals:
  - Build trust in technology through norms
  - Raise concern for security of the supply chain
  - Emphasize importance of public/private collaboration

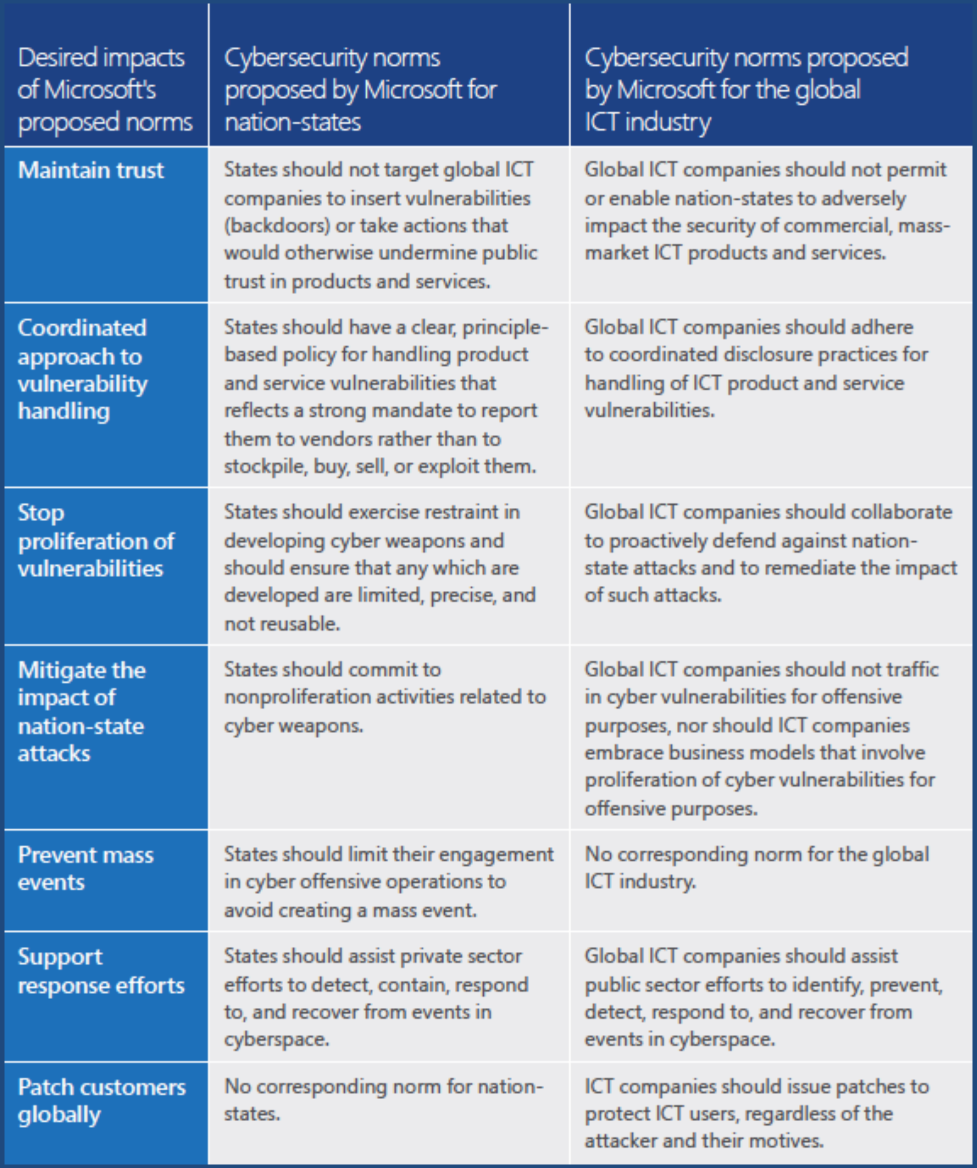
* "The need for a Digital Geneva Convention" by Brad Smith, Microsoft President & Chief Legal Officer https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ , 2017

Microsoft Norms Categories



Categories	Actors	Objectives	Actions	Impacts	Forums
Offensive norms	Nation-states, particularly militaries and intelligence agencies	Reduce conflict between states, lower the risk that offensive operations escalate, and prevent unacceptable consequences	Exercise self-restraint in the conduct of offensive operations	Mitigate unacceptable impacts of ICTs by governments	Inter-governmental bodies
Defensive norms	Public and private sector cyber defense teams	Manage cybersecurity risk through enhanced defenses and incident response	Collaborate among defenders (such as sharing information and best practices, coordinating responses)	Protect government, enterprise, and consumer users of ICT	Cyber defense organizations
Industry norms	Global ICT companies	Deliver secure products and services	Support defense and refrain from offense	Protect ICT users and enhance their trust in technology	Global ICT market and emerging leadership venues

Microsoft Norms



Desired impacts of Microsoft's proposed norms	Cybersecurity norms proposed by Microsoft for nation-states	Cybersecurity norms proposed by Microsoft for the global ICT industry
Maintain trust	States should not target global ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.	Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services.
Coordinated approach to vulnerability handling	States should have a clear, principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.	Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.
Stop proliferation of vulnerabilities	States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.	Global ICT companies should collaborate to proactively defend against nation-state attacks and to remediate the impact of such attacks.
Mitigate the impact of nation-state attacks	States should commit to nonproliferation activities related to cyber weapons.	Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.
Prevent mass events	States should limit their engagement in cyber offensive operations to avoid creating a mass event.	No corresponding norm for the global ICT industry.
Support response efforts	States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.
Patch customers globally	No corresponding norm for nation-states.	ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.

GCSC Norms Developments

- 2017 – Global Commission on the Stability of Cyberspace (GCSC) launched by Dutch to enhance the international stability of cyberspace.
- 2018 – GCSC Singapore Norm Package:
  - Avoid Tampering
  - No Commandeering of ICT Devices into Botnets
  - Create a Vulnerabilities Equities Process
  - Reduce and Mitigate Significant Vulnerabilities
  - Basic Cyber Hygiene as Foundational Defense
  - No Offensive Operations by Non-State Actors

Recent Developments

- Charter of Trust for a Secure Digital World*
  - Launched by Siemens at Munich Security Conference 2018
  - Complementary to Microsoft's Digital Geneva Convention

* https://www.cyberscoop.com/siemens-cybersecurity-charter-of-trust-airbus-dxp-cyber-norms/

Charter of Trust Initiative*

- Calls for binding rules and standards to build trust in cybersecurity & advance digitalization.

- AES
- Allianz
- Airbus
- Atos
- Cisco
- Daimler
- Dell Technologies
- Deutsche Telekom
- Enel
- IBM
- Mitsubishi Heavy Industries
- NXP
- Siemens
- SGS
- Total
- TÜV Süd

* Launched at 2018 Munich Security Conference by Siemens
https://www.siemens.com/press/en/feature/2018/corporate/2018-02-cybersecurity.php

Charter of Trust
Principles

1. Build in security by default
2. Assign responsibility throughout supply chain
   - Identity and access management
   - Encryption
   - Continuous protection
3. User-centricity
   - Be trusted partner to user throughout life cycle
4. Firms and policymakers cooperate, innovate and adapt to new threats

Charter of Trust
Principles

5. Add cybersecurity courses to school curricula
6. Develop critical infrastructure/IoT certifications
7. Share new insights and incident data
8. Promote multilateral collaboration on regulation and standardization
9. Drive joint initiatives to implement principles

Open-Ended Working Group

- In 2019 UNGA the created Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)
- OEWG proposed by Russian Federation as alternative to GGE* small committee meetings.
  - OEWG invites all states to participate
  - Recommendations may diverge from GGE's on applicability of principles of international human law.

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

Review

- The norms development process
  - Evolution, emergence, framing
- Phases of cyber norms development
  - Contestation, Translation, Emergence, Internationalization
- Role of US (Secretary Kerry) and UN GGE
  - Bilateral agreements
- Microsoft norms
- GCSC and EWI joint norms universalization project
- Charter of Trust
- OEWG vs GGE outcomes