Internet governance: A confused landscape

David D. Clark
MIT CSAIL
April, 2016
Only a few institutions get attention

- Most of the attention (and contention) around Internet governance focuses on a few groups:
  - ICANN
  - ITU
  - IETF
  - Internet Governance Forum (IGF)
  - National regulators (e.g., the FCC in the U.S.)

- But what role do they actually play?
Governance roles

IETF:
- Setting standards: a critical role.
- Not business practices, policy, etc.
- Self-defined, constrained role.

ITU:
- Little role, at the moment.
- They want a role.
  - WCIT-2012
- Only relevant to international issues.

FCC:
- Network neutrality.
  - Disputed authority in the U.S.

IGF
- A venue for conversations.
ICANN

• Perhaps the most visible (and disputed) governance organizations.
    • Now oversight is being re-defined.
  – Responsibility for IP addresses.
    • But work actually done by the Regional Internet Registries.
  – Responsibility for the Domain Name System
    • In particular, the top-level domains.
  – Actually, a very narrow remit.
What keeps the Internet going?

• Operational groups like the North American Network Operators’ Group (NANOG)
  – Network engineers meet to discuss pragmatic issues of the day.
  – A bottom-up, self-organized group.
  – Nobody gave them the job, they just took it.
  – Its critical role—developing social capital.
    • The magic ingredient? Beer.

• Beer is what keeps the Internet going.
My topic today: security

• Security is a critical issue for the future of the Internet.

• So, what governance institutions are in charge of Internet security?
  – None of the above... (Slight overstatement)

• What institutions do attempt to govern cyber-security?
  – Some data from a MS thesis by Cecilia Testart, a graduate student in my group.
Finding the institutions

• Start with a venue with diverse participation.
  – IGF
• Study the transcripts of all the sessions.
  – Use automated tools.
• See what people mean when they use the word “security”, and see what institutions they mention.
  – Then see how they define themselves.
• Follow the leads.
  – A sort of snowball sample method.
Where did she end up?

• Define “governance” broadly:
  – Is the institution shaping Internet security?

• 120+ institutions and counting.
  – Never find them all, but an interesting (and hopefully representative) sample.

• Seems, if anything, “over-institutionalized”
  – And yet, security is a persistent problem.

• Why so many, and what do they do?
Some random examples

- Governments
  - Legislature
  - Executive branch
- NSA, GCHQ, etc.
- FCC, FTC, DoJ, DoS, DHS
- EC directorates (5)
- OECD, G8
- Council of Europe
- European Data Protection Supervisor
- National Cyber Defense Center Germany
- Ministry of Administration and Digitization of Poland
- Shanghai Cooperation Organization

- Korean Internet and Security Agency
- National Cyber Security Alliance
- Global Institute for Cybersecurity + Research
- EU Institute for Security Studies
- CERTs
  - CC, EU, ICS, etc.
- IETF, ETSI, IEEE, ISO, ODCA, W3C
- M3AAWG, Spamhaus
- Financial Sector Information Sharing and Analysis Center
- Google, McAfee, Verizon, Mozilla, Symantec
- The Open Group
First hint—define security

• “Security” is not a well-defined objective.
  – Just a high-level aspiration.

• There is sub-structure to the goal of security.
  – And once we unpack the concept, we find conflict and tension among the sub-goals.
  – Security is about balance, not perfection.
Other features

• Focus on industry (or interest) sector.
• Different origins.
• Different methods of operation.
• Different regions of the world.
Classifying institutions

<table>
<thead>
<tr>
<th>Cyber Security Aspects</th>
<th>Activity Sectors</th>
<th>Jurisdictions</th>
<th>Institution Characteristics</th>
<th>Governance Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Emergency Response Team</td>
<td>Intelligence</td>
<td>United States</td>
<td>Forum</td>
<td>For Profit</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Software and Service Provider</td>
<td>Europe</td>
<td>Information Sharing</td>
<td>Not-for-Profit</td>
</tr>
<tr>
<td>Cyber Defense</td>
<td>Internet Policy</td>
<td>Other Regions</td>
<td>Working Group</td>
<td>Government</td>
</tr>
<tr>
<td>Cyber Security Research</td>
<td>Financial Sector</td>
<td></td>
<td>Consumer Oriented</td>
<td>Treaty Organization</td>
</tr>
<tr>
<td>Computer Security</td>
<td>Online Services</td>
<td></td>
<td>Economic Focus</td>
<td></td>
</tr>
<tr>
<td>Data Protection</td>
<td>Network Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>Internet Governance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>Telecommunications</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Different aspects of security

The Public Sector (Governments and international institutions) and private actors (for profit and not-for-profit) focus on different areas of cyber security.
Specialization

Most institutions seem to play just one role.
Institutional alternatives

• Many different roles, modes of operation, etc.
  – Suggests why the landscape is so cluttered.

• But with so many small players, is there any leadership?
  – Clear that “nobody is in charge”.

• Where can leadership come from?
  – Top down? By what authority?
    • Internet is built by private sector.
  – Bottom up? Authority has to be earned, and leads to distrust.
Why is security hard?

• Not a simple technical problem.
• What are some important barriers to progress?
  – Incentives and externalities.
  – Coordination problems and “first mover disadvantage”.
  – Issues of global scope.
  – Lack of trust.
• In this context, how could a “leadership institution” emerge?