Cyberspace & Digital Diplomacy

Kenny Huang, Ph.D. 黃勝雄博士

CEO & Director of the Board, TWNIC

Executive Council, APNIC
huangk@twnic.net.tw
Mar 23 2018
Definition of cyberspace

- Definition: cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. (Kuehl 2009)

- Concept of cyberspace: it is the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place. (Clark, MIT 2010)
David Clark’s views of cyberspace

- The **people** who participate in the cyber-experience—who communicate, work with information, make decisions and carry out plans, and who themselves transform the nature of cyberspace by working with its component services and capabilities.

- The **information** that is stored, transmitted, and transformed in cyberspace.

- The **logical building blocks** that make up the services and support the platform nature of cyberspace.

- The **physical** foundations that support the logical elements.

- Model to understand control points of the cyberspace and internet
Aspects of David Clark’s Model

1. The physical foundations of cyberspace are important - cyberspace is a real artifact build out of real elements. But the nature of cyberspace derive more from the decisions made at the logical level than the physical level.

2. Cyberspace, at the logical level, is thus a series of platforms, on each of which new capabilities are constructed, which in turn become a platform for the next innovation.

3. Information layer: many forms of information, video, music, records of businesses, transaction records, meta-data, static and dynamically created information, etc.

4. Top layer: people, not just passive users of cyberspace, but people that define its character by the ways they choose to use it.
Nazli Choucri’s view of cyberspace

- Origin of the term: Willian Gibson (Neuromancer) proposed it as a combination of cybernetics and space
- Cyberspace is a venue that allows users to engage in activities conducted over electronic fields whose spatial domain transcend territorial, governmental, social and economic constraints.
- Cyberspace is becoming heavily contested, colonized and reshaped by governments, militaries, and private corporate and civic networks.
Cyberspace & international relations

- Cyberspace is destroying the link between geographic location and
  - The power of local governments to assert control over online behavior;
  - The effects of online behavior on individual or things;
  - The legitimacy of the efforts of a local sovereign to enforce the rules apply
- The construction of cyberspace is a globalizing phenomenon, irrespective of how one views the globalization process itself.
Characteristics of cyberspace

- Temporality - replaces conventional temporality with near instantaneity
- Physicality - transcends constraints of geography or physical location
- Permeation - penetrates boundaries and jurisdictions
- Fluidity - manifests sustained shifts and reconfigurations
- Participation - reduces barriers to activism and political expression
- Attribution - obscures identities of actors and links to action
- Accountability - bypasses mechanisms of responsibility
- Examples of cyber-companies: Uber, Airbnb, Facebook and Google
Cyberspace and physical world

WELCOME TO UBERVILLE
What is cyberspace governance

- Cyber activities: complex and distributed landscape
- Encompasses debates in technical, economic, political, social, military, law enforcement and intelligent areas
- Management of cyberspace could be viewed as a broad set of rules, norms, institutions and processes.
- Cyberspace is a true domain on a par with Land, Air, Space, and Sea in military viewpoint (e.g.: apply the basic questions of the Principles of War)
- Cyber governance includes the establishment of formal and informal norms for state behavior and non-state actors, better legal mechanisms for addressing cross-border cybercrime, transparent national legislation for law enforcement, and endorsement of the need for encryption to protect the integrity of data.
Aspects of cyber governance

- Considerable insecurity in the cyberspace: barriers to enter are low and there is an asymmetry between offense and defense costs;
- Governments manage national spectrum allocation within the framework of UN-ITU;
- In the UN charter, the Laws of Armed Conflict (LOAC) provide a framework to manage security and espionage problems;
- In practice there are many areas of private and public governance;
- Providing security is a classic function of government;
- Rampant cyber espionage activities;
- Governments want to protect the internet for the benefit of their societies, but also want to protect societies from what might come through the internet: practice of censorship (e.g.: Google, Twitter, Facebook, etc)
What is cyberspace governance

- Mapping of cyber governance using regime theory.
- Regimes are the principles, norms, rules and procedures that govern issue areas in international affairs.
- A regime complex is a loosely coupled set of regimes.
- While there is no single regime for governance of cyberspace, there is a set of loosely coupled norms and institutions involved.
- Governments and non-state actors cooperate and compete for power in cyberspace (e.g., US vs. China; Europe vs. Google).

- Governance map:
  - Indicate the extend and wide range of actors and activities
  - Separation between technical function of connectivity from the rest
  - Layers and domains much broader than ICANN functions
Global cyber activities

Joseph Nye, May 2014
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTA</td>
<td>Anti-Counterfeiting Trade Agreement</td>
</tr>
<tr>
<td>ARF</td>
<td>Association of Southeast Asian Nations Regional Forum</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>DAC</td>
<td>Development Assistance Committee (OECD)</td>
</tr>
<tr>
<td>EBRD</td>
<td>European Bank for Reconstruction and Development</td>
</tr>
<tr>
<td>EFF</td>
<td>Electronic Frontier Foundation</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum for Incident Response and Security Teams</td>
</tr>
<tr>
<td>&quot;Five Eyes&quot;</td>
<td>Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States</td>
</tr>
<tr>
<td>G8</td>
<td>Group of Eight</td>
</tr>
<tr>
<td>G20</td>
<td>Group of Twenty</td>
</tr>
<tr>
<td>GGE</td>
<td>Group of Governmental Experts (UN)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUCCI</td>
<td>Global Undersea Communications Cable Infrastructure</td>
</tr>
<tr>
<td>IAB</td>
<td>Internet Architecture Board</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communications technology</td>
</tr>
<tr>
<td>ICT4D</td>
<td>Information and Communication Technologies for Development</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IGF</td>
<td>Internet Governance Forum</td>
</tr>
<tr>
<td>IMF</td>
<td>International Monetary Fund</td>
</tr>
<tr>
<td>ISOC</td>
<td>Internet Society</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITRs</td>
<td>International Telecommunication Regulations</td>
</tr>
<tr>
<td>IWWN</td>
<td>International Watch and Warning Network</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organization for Security and Co-operation in Europe</td>
</tr>
<tr>
<td>RIRs</td>
<td>regional Internet registries</td>
</tr>
<tr>
<td>SCU</td>
<td>Shanghai Cooperation Organisation</td>
</tr>
<tr>
<td>SCUs</td>
<td>telecommunications company</td>
</tr>
<tr>
<td>UNGA</td>
<td>United Nations General Assembly</td>
</tr>
<tr>
<td>WSIS</td>
<td>World Summit on the Information Society</td>
</tr>
</tbody>
</table>
Newcomers in Internet governance regime: acronyms & role play
Cyberspace governance is difficult because of the newness and volatility of technology.

Dimensions for comparing cyber issues: depth, breadth, fabric and compliance

- Depth refers to the hierarchical coherence of a set of rules or norms (e.g., domain names).
- Breadth refers to the scope of the numbers of state and non-state actors that have accepted a set of norms (e.g. Budapest convention, 42 states).
- Fabric refers to the mix of state and non-state actors in an issue area (e.g. laws of war).
- Compliance refers to how widespread is the behavioral adherence to a set of norms (e.g., domain names & protocols).
### Some Issues in the Cyber Regime Complex

<table>
<thead>
<tr>
<th>Issue</th>
<th>Depth</th>
<th>Breadth</th>
<th>Fabric</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS/standards</td>
<td>High</td>
<td>High</td>
<td>Loose</td>
<td>High</td>
</tr>
<tr>
<td>Crime</td>
<td>High</td>
<td>Medium</td>
<td>Mixed</td>
<td>Mixed</td>
</tr>
<tr>
<td>War/sabotage</td>
<td>Medium</td>
<td>Low</td>
<td>Tight</td>
<td>Low</td>
</tr>
<tr>
<td>Espionage</td>
<td>Low</td>
<td>Low</td>
<td>Mixed</td>
<td>Low</td>
</tr>
<tr>
<td>Privacy</td>
<td>Medium</td>
<td>Low</td>
<td>Mixed</td>
<td>Mixed</td>
</tr>
<tr>
<td>Content control</td>
<td>Low</td>
<td>Low</td>
<td>Loose</td>
<td>Low</td>
</tr>
<tr>
<td>Human rights</td>
<td>Medium</td>
<td>Medium</td>
<td>Loose</td>
<td>Low</td>
</tr>
</tbody>
</table>
Evolution of cyberspace governance

- Evolution of cyber complex regimes:
  - Realists: regimes are created and sustained by the most powerful state.
  - Liberal institutionalism: emphasizes the rational self-interest of states seeking the benefits of cooperative solutions to collective action problems.
  - Constructivist set: emphasizes cognitive factors, such as how constituencies, groups and social movements change the perception and organization of their interests over time

- Compared to other domains (e.g.: the 1968 Non-Proliferation Treaty of nuclear weapons) the situation in cyber is more complex by the much greater roles of a diverse set of private and non-profit actors responding to rapid technological, social (i.e., generational cognitive evolution), political and economic change.
Cyberspace governance

Source: Chehade & Company, 2016
1. Informal Industry Norms and Practices
2. Coordination Services Firms
3. Production Alliance
4. Cartel
5. Business Associations
6. Private Regime

### Public Goods Governance Models

<table>
<thead>
<tr>
<th>Governance Capability &amp; Capacity for Public Goods</th>
<th>Non-state Actors</th>
<th>Governments</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

|------------------|-------------------------|-------------------------------------|--------------------------|---------------------------------|

- Delegation (Tanja, Borzel, 2007)

Source: edited by Dr. Kenny Huang

Reference:
- Knill, 2002
- Tanja, Borzel, 2007
Governance With/Without Government

Governance by government

Public regulation
No involvement of private actors

Consultation/co-optation of private actors
Participation of private actors in public decision-making
(for example private actors as members of state; delegation; outsourcing)

Co-regulation/co-production of public and private actors
Joint decision-making of public and private actors
(for example social partners in tripartite conciliation; public-private partnerships)

Delegation to private actors
Participation of public actors
(for example contracting-out; standard-setting)

Governance with government

Private self-regulation in the shadow of hierarchy
Involvement of public actors
(for example voluntary agreements)

Public adoption of private regulation
Output control by public actors
(for example erga omnes effect given to collective agreements of social partners)

Private self-regulation
No public involvement
(for example private regimes; social partner autonomy)

Governance without government

source: Tanja Borzel, 2010
The Shadow of Hierarchy

source: Tanja Borzel, 2010
The shadow of hierarchy
- The state threatens - explicitly or implicitly - to impose binding rules or laws on private actors in order to change their cost-benefit calculations in favor of a voluntary agreement closer to the common good rather than to particularistic self-interests.

Implications to governments
- the higher the government’s capacity for hierarchical policy-making, the fewer incentives it has to cooperate with non-governmental actors.
- weak states are unlikely to engage in governance with non-state actors because they might fear a loss of autonomy

Implications to non-state actors
- it generates important incentives for cooperation for non-state actors
Monopoly and Regulatory Competition Model

- **Monopoly and anti-competition**
  - The main problem with private self-regulation is the anti-competitive incentives flowing from their monopoly power

- **Restrict supply of the professional service**
  - Private self-regulation will have been granted for monopolistic control for a certain territory, thus have the power to restrict supply of their professional service

- **Regulatory competition model**
  - Subjecting these organizations to competition from other self-regulatory organisms might stimulate more welfare enhancing behavior (Kay and Vickers, 1990)
Limitations of Self-Regulatory Competition

- **Race to The Bottom mechanism**
  - the states compete with each other as each tries to underbid the others in lowering taxes, spending, regulation...so as to make itself more attractive

- **Limited mobility**
  - the location decision of professionals is much more dependent on cultural and social ties

- **Negative externalities**
  - regulatory competition between professional standards is the potential of negative externalities flowing from low quality service provision.
Multistakeholder Model

- **Multilateral Model**
  - multiple countries working in concert on a given issue
  - the practice of coordinating national policies in groups of three or more states

- **Multistakeholder Model**
  - an organizational framework or structure which adopts the multistakeholder process of governance or policy making, which aims to bring together the primary stakeholders such as businesses, civil society, governments, research institutions and non-government organizations to cooperate and participate in the dialogue, decision making and implementation of solutions to common problems or goals.
  - A stakeholder refers to an individual, group or organization that has a direct or indirect interest or stake in a particular organization
## Club vs. network diplomacy

<table>
<thead>
<tr>
<th></th>
<th>Number of players</th>
<th>Structure</th>
<th>Form</th>
<th>Transparency</th>
<th>Main purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Club</td>
<td>Few</td>
<td>Hierarchy</td>
<td>Mostly written</td>
<td>Low</td>
<td>Sign agreements</td>
</tr>
<tr>
<td>Network</td>
<td>Many</td>
<td>Flatter</td>
<td>Mostly oral</td>
<td>High</td>
<td>Increase flows</td>
</tr>
</tbody>
</table>

Source: Oxford Handbook of Modern Diplomacy
The empowerment of the public state to non-state diplomacy = Gov’s diplomatic cooperation with transnational civil society actors

Source: Oxford Handbook of Modern Diplomacy
Digital diplomacy : facet of digital tools/social media

- **Basic definition**
  - The use of digital technologies in support of diplomatic objectives

- **Impact of digital tools / social media** *(twiplomacy, 2016)*
  - **Twitter**
    - % of UN member states: 90%
    - Audience: 325 million
  - **Facebook**
    - % of UN member states: 88%
    - Audience: 255 million

- **Implication to MFA**
  - Driven by the opportunity to engage with million of people at the minimal costs
  - use of the platforms for engaging with communities and foreign public, communication with nations in times of international crises.
Tradeoff between the Internet and lifestyle

% of respondents willing to give up a lifestyle habit for a year instead of the Internet

Source: Boston Consulting Group, 2012
Inter-professional communication
What is the best timing for digital tools and digital diplomacy

Source: Diplo Foundation, 2015  Modelled on the Gartner Hype Cycle
Digital tools for digital diplomacy
Outward focused MFA digital activities

- Public diplomacy, advocacy, dialogue
- Strategic communications, branding, PR campaigns
- Collaborative intelligence, innovation, problem-solving
- Trade and investment promotion
- Contract development, relationship building, network formation
- Outreach and constituency-building
- Travel advice and consular information
- Representation in cyberspace
Inward focused MFA digital activity

- Knowledge access, generation, accumulation
- Development of ideas, analysis, projects
- International policy formulation
- Information sharing and internal publishing
- Telework, distance learning, language training and simulations
- Employee in-reach and internal communications
- Channels for reform, dissent, criticism
- Institutional memory
Benefits for MFA from going digital

- Effectiveness - MFA can better connect and communicate with new players in international society
- Efficiency - MFA can reach much larger audiences and capture a range of related benefits
- Leverage - MFA can use the new media to play to the strengths of national image and reputation while minimizing the constraints associated with capacity or security limitations
MFA digital tools engagement

- 140 MFA have established an online presence
- 38% use Twitter
- 37% use Facebook
- 28% use YouTube
- 6% have a blog on their main website

Source: Diplo Foundation, 2015
Twitter cyberspace

250 accounts of world leaders

128 heads of states on Twitter

Source: Diplo foundation, 2015
MFA on social media

<table>
<thead>
<tr>
<th>Rank</th>
<th>Social Media</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,2,3</td>
<td>Twitter</td>
<td>Twitter ranks first as the most commonly used social network by foreign ministries, Facebook#2, YouTube#3</td>
</tr>
<tr>
<td>16%</td>
<td></td>
<td>The percentage of foreign ministries who do not yet have a website</td>
</tr>
<tr>
<td>41K</td>
<td>YouTube</td>
<td>The highest number of subscribers to a foreign ministry, YouTube channel, belonging to US Dept. of State</td>
</tr>
<tr>
<td>4.6M</td>
<td>Twitter</td>
<td>The foreign minister with the highest number of followers on Twitter (India’s MFA)</td>
</tr>
<tr>
<td>320M</td>
<td>Twitter</td>
<td>The number of monthly active users on Twitter</td>
</tr>
</tbody>
</table>

Source: Diplo foundation, 2016
@JustinTrudeau
Canada's Justin Trudeau is the rising social media darling, active on most social media channels. Since taking office the Canadian Prime Minister tweets in English and French, although most of the heavy social media lifting is done by his team. His friendly attitude has recently taken a hit after elbowing his way through a parliamentary debate. But then he used Twitter to apologize.

@Erna_Solberg
Kudos to the Norwegian Prime Minister, who is among the most conversational world leaders on Twitter and tweets personally despite suffering from dyslexia and making the occasional spelling mistake. We wish she would write more in English. PS.: we don't mind the typos.

@NarendraModi
No one can ignore the meteoric rise of Indian Prime Minister Narendra Modi and his superb use of the platform which has given him an enormous social media footprint. Our prediction is that he will be the most followed world leader by 2017.

@TaaviRoivas
Estonia's 36-year old Prime Minister has proudly tweeted how easy it is to securely sign documents, pay taxes and e-vote in the most digital country in the world. Next up: cast your vote with a Direct Message on Twitter. #Seriously
Since last year he is wearing a tie on his Twitter profile.
The power of hashtag

Although critics point out the laziness of this use of hashtag activism, some of the 6.1 million users of #BringBackOurGirls defended the trending topic, offering their own criticism of those who shame others for not meeting their standards of awareness.
EU digital diplomatic strategies

Source: European Commission
Different platforms, different audiences

- General interest
- Students and young people
- Organisations and campaigns
- Journalists
- Think-tanks
- NGOs
- Leaders
- Tech-savvy
- Political
- Professional
- Consultancies
- Researchers
- Staff
- General interest
- Students and young people
- Brings together audiences from all platforms
EU digital diplomacy action areas

Source : European Commission
EU commissioners engaging experience

2010

7 EU Commissioners
11 Spokespersons

7 Commissioners

2014

22 EU Commissioners
25 Spokespersons

Average Daily potential reach: 128 million users

10 Commissioners

Total number of fans: 93K

Source: European Commission
Putting digital diplomacy in place
World bank digital tools engaging experience

- 2005 - first blog launches
- 2008 - blogging goes mainstream, social media pioneers
- 2010 - social media policy endorsed / adopted
- 2011 - governance, crowdsourced campaigns, Arabic blog, Chinese microblog
- 2013 - HR onboarding, shift from campaigns to conversations /streams
Misconceptions for digital diplomacy

- **misconception: digital technologies can grant extraordinary power**
  - Small and medium sized states: Sweden, Netherlands
  - E.g. MFA could positively shape the views of the global public, increase the diplomatic standing of the country in bilateral or multilateral context
  - Digital technologies can only support certain foreign policy objectives

- **misconception: ”going digital” is easy**
  - E.g. MFA can pursue their digital diplomatic ambitions with modest investments
  - Usually, MFAs have no clear direction or strategy to build their digital profile
Engage stakeholders require expertise and practice

Source: Makaira KK, Ko Fujii
Adopting digital tools in public diplomacy

- Adopt a step-by-step approach
- Define target audience
- Do not expect to control everything
- Allocate sufficient resources for the campaign
- Start with monitoring online commentary
- Create engaging content
- Disclose your identity and be sincere
- Attract users to your site
- Monitor your campaign in real time
Digital tools adoption for MFA

- One day
  - Learn how to use digital tools technically

- One month
  - Learn about organization and culture of digital tools, especially social media space

- One year
  - Use digital tools effectively
Communication is not good enough

- Flog message is not good enough
  - Users expect engagement
    - Getting message out but not responding to the feedback is counterproductive.

- Go beyond communication
  - Gather information
  - Assess public opinion
  - Communicate consular warnings

- Advance of the technologies
  - Big data, data mining technologies
  - Obtain real time information about terrorist attacks, natural disasters
  - MFAs need to pay more attention to the possibilities of new technologies (e.g., big data..)
Digital diplomacy operating model

**Propaganda Model**

- Stake Actors
- Audiences

**Engagement Model**

- Stake Actors
- Stakeholders

Source: Kenny Huang, Ph.D.
Digital diplomacy operating model

Reciprocity Model
Trade Agreement

Multi-stakeholder Model

Source: Kenny Huang, Ph.D.
2013年6月24日，第6次聯合國大會公布A/68/98文件

國家主權適用於國家所進行的資通訊技術相關活動（ICT-related activities），並適用於國家其領土內資通訊基礎設施的管轄權

資料來源：聯合國

正確選項：□ 管轄權
Country code top level domain world map

Source: Nominet
Positive externalities for digital diplomacy

<table>
<thead>
<tr>
<th>Positive Externalities</th>
<th>Outcome</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efficiency</td>
<td>Digital diplomacy improve MFA operational efficiency</td>
<td>MFA online presence, Advocacy, PR campaigns, Consular information</td>
<td></td>
</tr>
<tr>
<td>Innovation</td>
<td>Improve stakeholder engagement</td>
<td>Collaborative intelligence, Constituency building</td>
<td></td>
</tr>
<tr>
<td>Value chain rebuilt</td>
<td>Multistakeholder establish new regime, new governance &amp; business</td>
<td>New Internet governance model, New regime: DANE, RPKI, New collaboration: LEA &amp; RIR</td>
<td></td>
</tr>
</tbody>
</table>

Source: Kenny Huang, Ph.D.
New regime in cyberspace

- Identify key issue, collaborate with global stakeholders
- Explore potential solutions
- Standardize technological components with technical communities
- Group stakeholders as constituency and develop policy framework
- Engage broader stakeholders (stake/non-stake actors)
- Go beyond digital legacy
How about the future?

“Huh. So Iran just friended us on Facebook ... Like, do I accept?”