Conformity of Internet Peace Principles with the Policies of China and USA

July 3, 2018

KAIST Bright Internet Research Center
Young Yung Shin

Table of Contents

1. Introduction

- Cyber threats cause national insecurity, economic damage, social unrest
  - Cyberattacks, cyber crimes, election meddling, fabrication of information, fake news …

- Some progress made in cooperation for a secure cyberspace.
  - China and USA efforts are ineffective due to Internet's transnationality.

- Internet Peace Principles suggested as an international cyber security norm.

1. Introduction

- A staged implementation based on IPP

- Application of IPP to China and USA cybersecurity policies
  - Comparison of similarity and difference
    . Between IPP and the two countries cyber security policies
    . Between the two countries cyber security policies

- It emphasizes the importance of two countries' close cooperation for a staged implementation of IPP.

1. Introduction

❑ Scope of the research

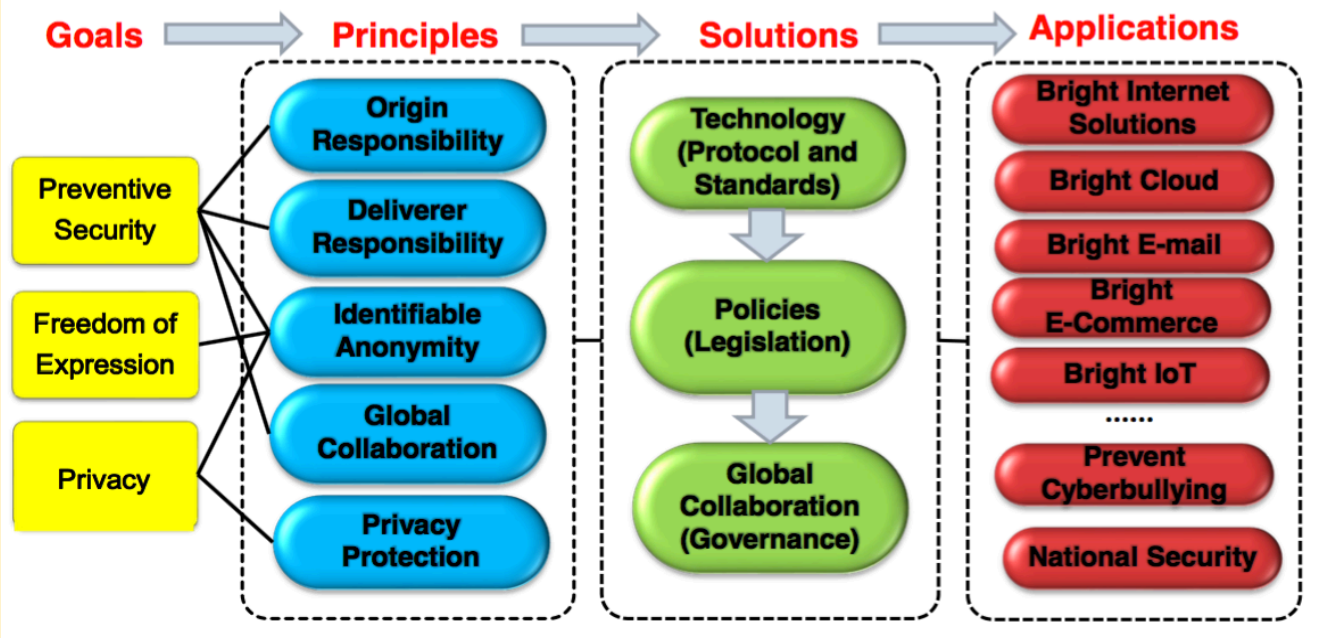
- **China** Cybersecurity Law (2017)
  National Cyberspace Security Strategy (2017)
  International Strategy of Cooperation on Cyber Security (2017)
  World Internet Conference in Wuzhen (2017)
  China and USA Agreement (2015)

- **USA** Cyberspace Policy Review (2009)
  Comprehensive National Cyberspace Initiative (2010)
  International Strategy for Cyberspace (2011)
  Department of State International Cyberspace Strategy (2016)
  Executive Order 13800 (2017)
  National Security Strategy of USA (2017)
  Department of Homeland Security' Cybersecurity Strategy (2018)

2. Bright Internet and Internet Peace Principles

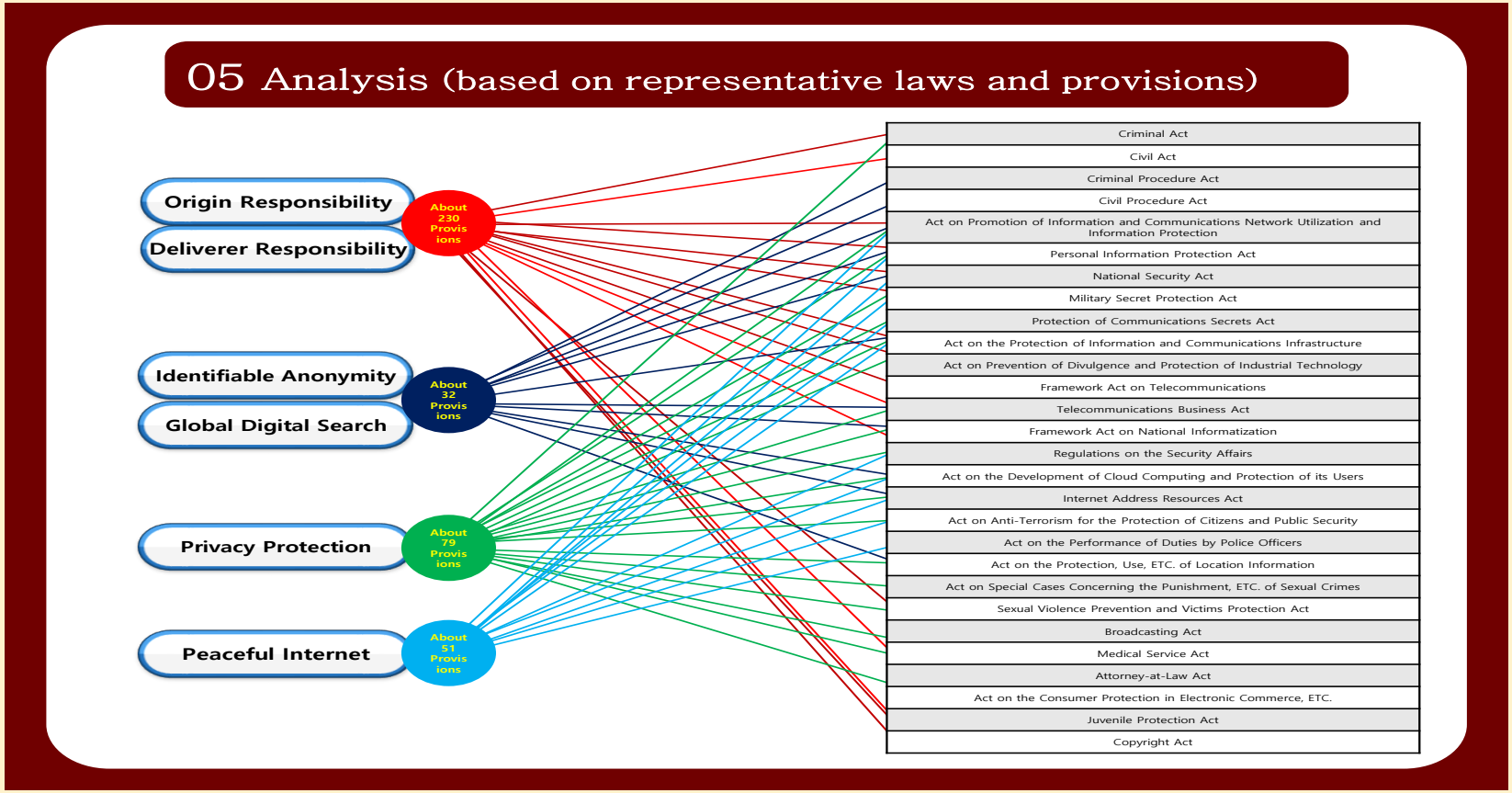
2.1 Bright Internet Principles

- Shifting paradigm from protective that a information receiver takes responsibility to preventive framework to preclude cybercrimes and track down the attackers.



2. Bright Internet and Internet Peace Principles

* Bright Internet and Internet Peace Principles Study in Korea



2. Bright Internet and Internet Peace Principles

2.2 Internet Peace Principles

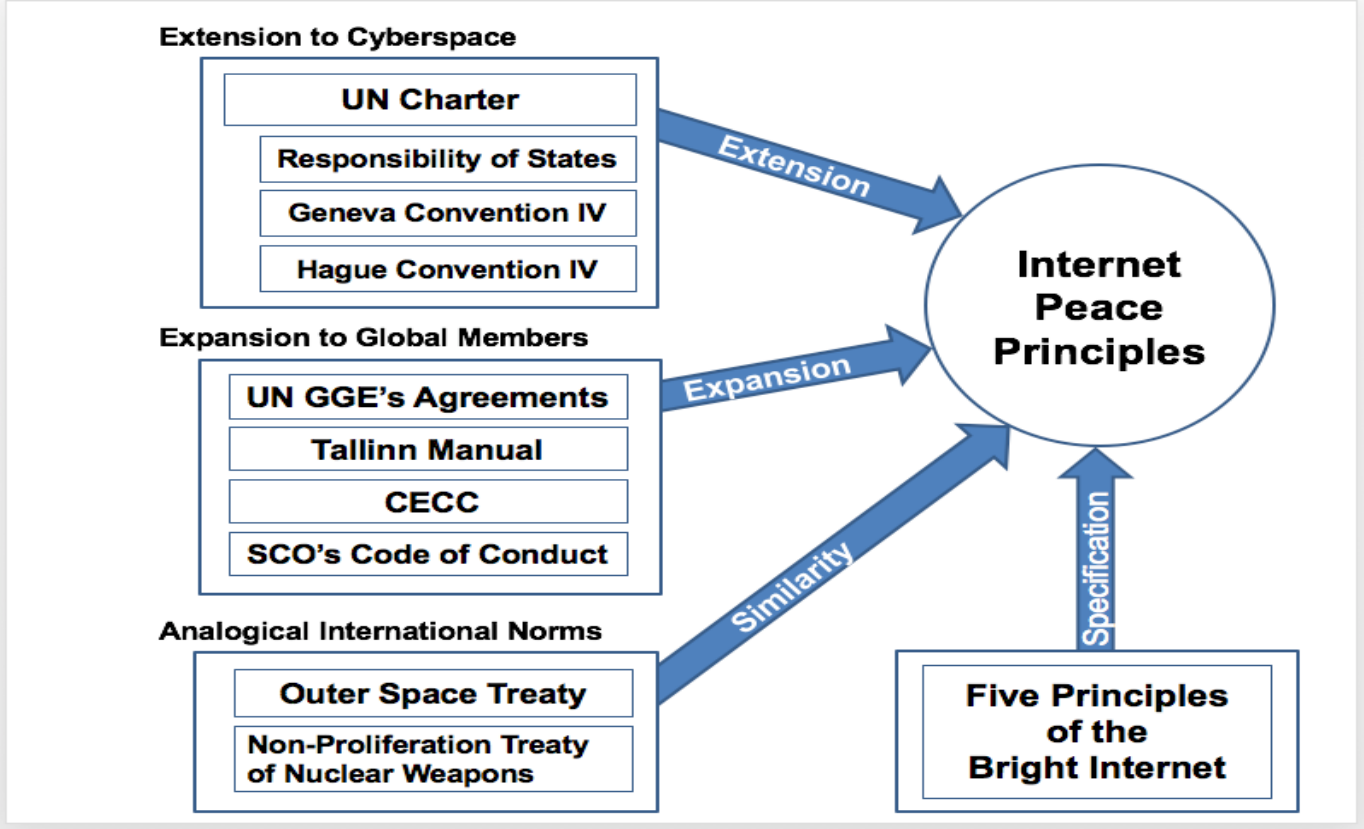
- Not using the Internet as a weapon for attacking other countries or as a means of detoured malicious cyberattacks.

- A preventive cybersecurity framework to deter SLCAs*
  = Bright Internet + Internet Peace Principles
  → Responsible states behavior in cyberspace

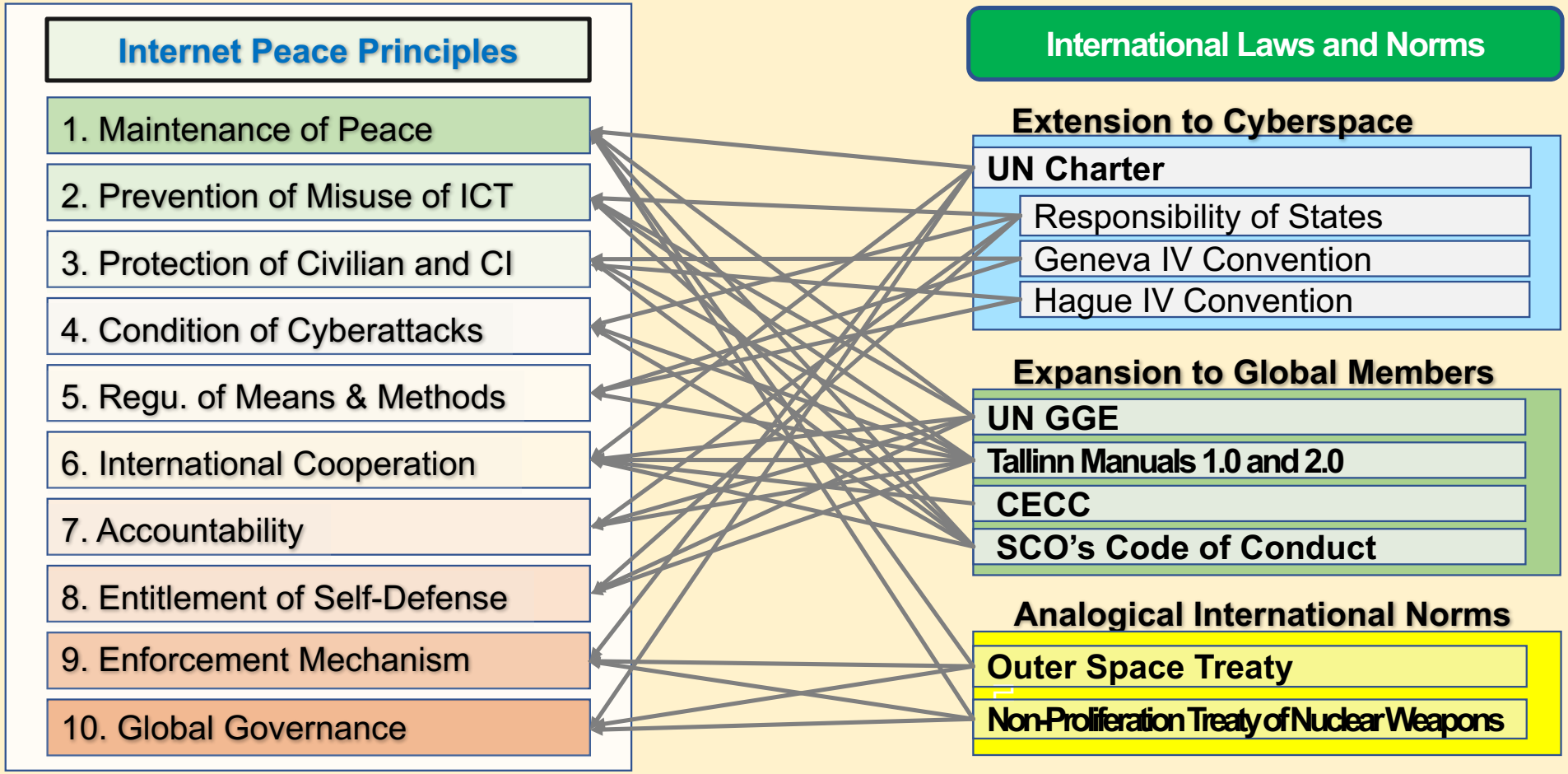
* State-Led Cyber Attacks

2. Bright Internet and Internet Peace Principles

2.3 Methodology for Internet Peace Principles



2.4 Ten Principles of the Internet Peace



3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle one*: *All states should maintain international peace and security in cyberspace.*

	China	USA
- Similarity or Difference	**Same**	
- Characteristics	- Safeguarding global peace, protecting peace as well as peaceful use of cyberspace ⓐ - Building a peaceful cyberspace ⓑ - Advocating the principles of peace in cyberspace and peaceful settlement of disputes ⓑ - Peace and stability in cyberspace ⓑ	- Achieving and maintaining a peaceful cyberspace environment ⓒ - Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace ⓓ
*References	ⓐ II and III-(2) of China National Cyberspace Security Strategy (NCSS) ⓑ Preface, Chap.II-1 and Chap.IV-1 of International Strategy of Cooperation on Cyberspace (ISCC)	ⓒ p.12 in Department of State International Cyberspace Policy Strategy (ICPS) ⓓ p.9 in International Strategy for Cyberspace (ISC)

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle two*: *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.*

	China	USA
- Similarity or Difference	**Same**	
- Characteristics	- Individuals and organizations must not engage in illegal entry, disruption, theft; must not provide programs, or tools, disrupting, stealing; where clearly knowing that others will engage in actions endangering network security, must not provide them with help. ⓐ - Illegal criminal activities should be tackled. ⓑ	- Protecting their own networks and information infrastructure to ensure they are secure, reliable, and resilient.ⓒ - Protect Federal Government Information Systems ⓓ - Protective measures for critical information ⓔ - Due diligence (domestic governance) ⓕ
*References	ⓐ Article 27 of China Cybersecurity Law (CCL) ⓑ III-2 ISCC	ⓒ p.4 in ICPS ⓓ p.3 in Department of Homeland Security Cybersecurity Strategy (DHSCS) ⓔ Executive order 13800 ⓕ p.10-11 in ISC

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle three*: *States should prohibit cyberattacks against critical infrastructure, innocent civilians and their facilities.*

	China	USA
- Similarity or Difference	**Same**	
- Characteristics	- All individuals and organizations shall be responsible for their unlawful activities in cyberspace. ⓐ - Protecting critical information Infrastructure and raising the awareness of critical information infrastructure protection ⓑ	- Extending cybersecurity into critical infrastructure domains ⓒ - Protecting their own networks and information infrastructure ⓓ - Protecting federal information systems, critical infrastructure, and other systems ⓔ
*References	ⓐ Articles 46-48,50,68-70 of CCL ⓑ Article 5 of CCL, IV-(3) of NCSS, and IV-8 of ISCC	ⓒ Initiative #12 of Comprehensive Cybersecurity Initiative (CNCI) ⓓ p.4 in ICPS ⓔ p.11 in DHSCS

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle four*: *States should prohibit the use of SLCAs except for legitimate self-defense and countermeasure purposes.*

	China	USA
- Similarity or Difference	**Similar but a little different in response**	
- Characteristics	- Adoption of all measures including military measures to uphold cybersecurity ⓐ - Developing cybersecurity defense means to safeguard national cybersecurity ⓑ - Militarization and deterrence buildup in cyberspace is not conducive to international security and strategic mutual trust, but enhances its defense capability to protect cybersecurity.ⓒ	- Appropriate response must be conducted through cyber means for deterring and responding to malicious cyber activity. ⓓ -'Prevent and disrupt criminal use of cyberspace' ⓔ
*References	ⓐ IV-(1) of NCSS ⓑ IV-(8) of NCSS ⓒ III-1 of ISCC	ⓓ p.22 in ICPS ⓔ P.15 in DHSCS

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle five: States should regulate the unlimited use of the means and methods of cyberwarfare.*

	China	USA
- Similarity or Difference	**Similar but a little different in response**	
- Characteristics	- China has no documented regulations, because it believes militarization and deterrence buildup in cyberspace is not conducive to international security and strategic mutual trust. ⓐ	- USA treats cyber as a domain of warfare. ⓑ - USA can lawfully and proportionately respond to an act that meets the threshold of unlawfulness of an armed attack. ⓒ
*References	ⓐ III-1 of ISCC	ⓑ US Defense Department Quadrennial Defense Report (2010) ⓒ US Cybersecurity Strategy (2011)

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle six: States should cooperate to exchange information and prosecute terrorists.*

	China	USA
- Similarity or Difference	**Same**	
- Characteristics	- Countries should work together to ensure cyber security through constructive consultation and cooperation. ⓐ - China will explore norms of behavior and concrete measures for international cooperation against cyber terrorism. ⓑ	- Confidence building through cooperation - Promoting cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships. ⓒ
*References	ⓐ III-2 of ISCC ⓑ IV-5 of ISCC	ⓒ p.18 in ISC

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle seven: The offending state should be held responsible for the consequence of its cyberattacks.*

	China	USA
- Similarity or Difference	**Same**	
- Characteristics	- Offending activities should be punished. ⓐ - When foreign institutions ~ engage in attacks that cause massive damage ~ legal responsibility is to be pursued. ⓑ	- US uses indictment and sanction against offending organizations or individuals. - Strengthening international partnerships for cybersecurity activities, policies, and opportunities ⓒ - Increase counter-terrorism cooperation ⓓ - Promoting an open, interoperable, secure, and reliable Internet through international collaboration ⓔ, ⓕ
*References	ⓐ III-(1), IV-(2), (6) of NCSS, and IV-5 of ISCC ⓑ Article 75 of CCL	ⓒ p.VI of Cyberspace Policy Review (CPR) ⓓ p.48 in NSS, ⓔ p.24 in DHSCS ⓕ p.7 in ISC ⓕ

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle eight: An cyberttacked state is entitled to request compensation and to take legitimate self-defense and countermeasures.*

	China	USA
- Similarity or Difference	**Different**	
- Characteristics The two countries mobilize all means including military in safeguarding national security	- China does not agree that *self-defense and International Humanitarian Law should apply to cyberspace, because it "would legitimize a scenario of war and military actions in the context of ICT*". ⓐ - Disconnection of the Internet ⓑ - Adopting all measures including military measures to unwaveringly uphold country's sovereignty in cyberspace ⓒ - Giving play to the important role of the military in safeguarding the country's sovereignty, security, and development interests in cyberspace ⓓ	- Designation of cyberspace as 5th domain - "The United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force." ⓔ - Appropriate response must be conducted through cyber means. ⓕ
*References	ⓐ UNGGE 5th Meeting Discussion ⓑ Article 58 of CCL	ⓔ 2012 Legal adviser at the State Department

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle nine: The UN may take effective collective measures for the prevention and removal of cyber security threat and for the suppression of cyberattacks considering a cyber blockade.*

	China	USA
- Similarity or Difference	**Similar but a little different in preference**	
- Characteristics	- China prefers UN-centric and state-centric problem solution, so various prevention measures and solution could be discussed through the UN. ⓐ	- USA is in favor of current international cybersecurity convention like Budapest Convention and UNGGE - USA considers various effective punishment measures ⓑ. Such as sanction, indictment, “Isolating governments that refuse to act as responsible partners in advancing hemispheric peace and prosperity.” ⓒ51
*References	ⓐ II-3, III-2, IV-2 of ISCC	ⓑ p.28 in NSS ⓒ p.51 in NSS

3. Comparative Analysis of China - USA's Cybersecurity Policy based on IPP

❑ *Principle ten: A forum such as BIG Summit and a governance body such as the BIGO are necessary to conduct research and to realize the implementation and verification of the BI and IPP.*

	China	USA
- Similarity or Difference	**Similar but a little different in preference**	
- Characteristics	- Setting up the World Internet Conference (Wuzhen international Conference) and other international conference to cooperate ⓐ, ⓑ - Establishing multilateral approach governance ⓐ - UN-centric Internet Global Governance ⓐ - Supporting the United Nations to play a leading role ⓐ	- Preference for CECC, development of GGE - Multi-stakeholder approach - Active engagement in key organizations, such as ICANN, IGF, ITU, the UN ⓒ - Encouraging widespread adoption of voluntary norms of responsible state behavior in peacetime ⓓ
*References	ⓐ IV-(9) of NCSS ⓑ IV-3 of ISCC	ⓒ p.41 in National Security Strategy of USA (2017) ⓓ p.24 in DHSCS

4. Evaluation of Application of IPP to the Two Countries' Policy

4.1 Similarity and difference between IPP and the Two Countries' Policy

❑ **Similarity**

- IPP and the two countries' policy shared a similar recognition of cyber threats and a related cybersecurity policy.

- China is closer to IPP than USA in cybersecurity measures.
  . State-centric, cyberspace sovereignty, UN-centric

- USA is closer to IPP than China in state's responsibility.
  . Attacking country's accountability and attacked country's entitlement

→ Many similarities increase the possibility of establishment of global cyber norm and show the relevance of IPP as a global cybersecurity norm.

4. Evaluation of Application of IPP to the Two Countries' Policy

4.1 Similarity and difference between IPP and the Two Countries' Policy

❑ **Difference**

- IPP is more focused and detailed than two countries' cybersecurity policy on responsible state behavior.

. Limited use of SLCAs (Principle 4)

. Regulation of unlimited use of cyber means and methods (Principle 5)

. Attacking states responsibility and Attacked states entitlement (Principles 7&8)

→ Those issues could be discussed in the future for appropriate state behavior.

4. Evaluation of Application of IPP to the Two Countries' Policy

4.2 The Necessity and Prospect for China–USA Cooperation

(1) Cooperation for economy and national security

- China and US worry that there is no responsible state behavior norm.
- Economic damage: IP stealing cost $2,250 – 6,000 billion (0.8% of Global GDP) in 2018
- China needs USA's advanced and high technology.
- USA requires markets for its cutting-edge technology.

(2) Responsibility as a Leader Country

- Obligation to provide principles for safe and trustable cyberspace
- It will be desirable for China and USA to establish a commonly acceptable global cyber norm based on IPP.

4. Evaluation of Application of IPP to the Two Countries' Policy

4.3 Similarity and Difference of the Two Countries' Cybersecurity

❑ Similarity comes from each country's vulnerability and cybersecurity against it.

- Peace and security in cyberspace, Prevention of misuse of ICT,
- Protection of civilians and infrastructure, International cooperation, etc.

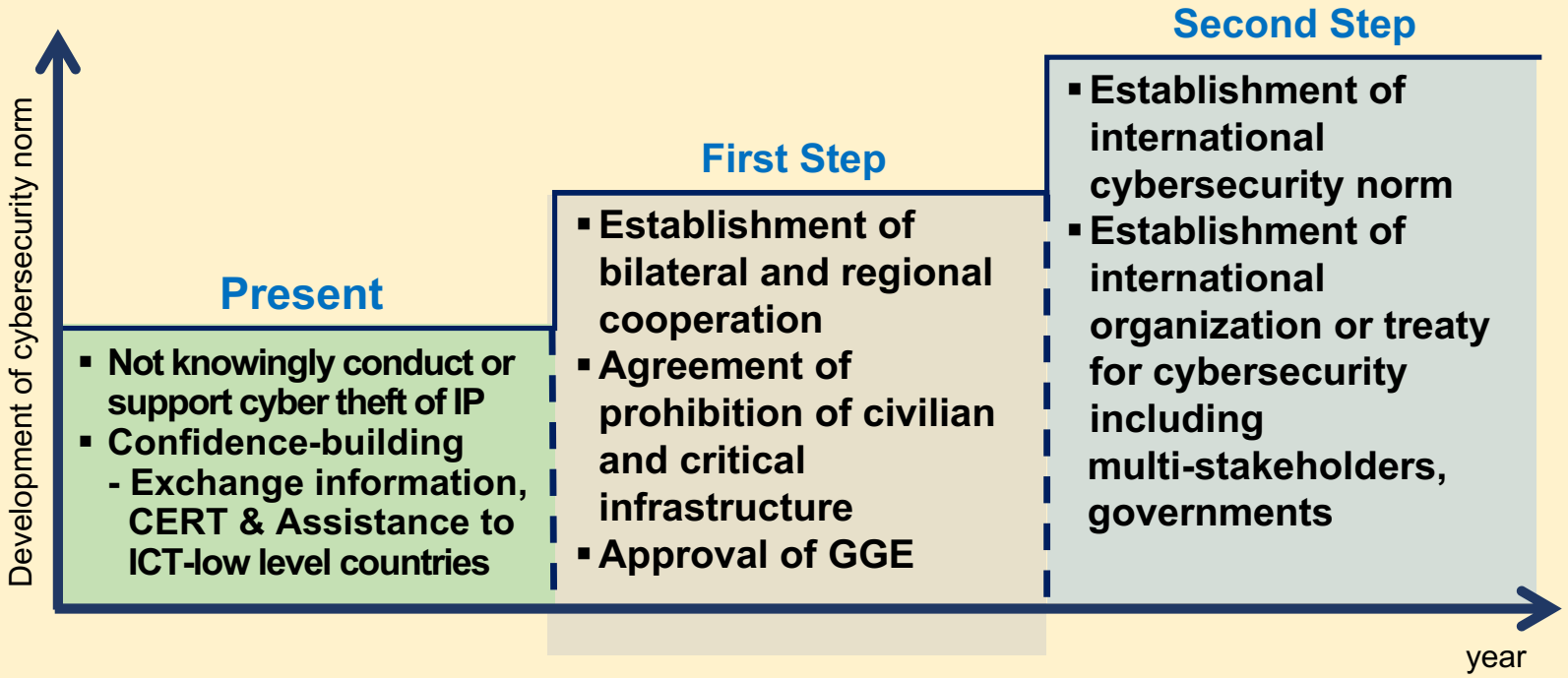
→ A lot of similarities expedite cooperation and the necessity of common ground like international cybersecurity norm.

❑ Differences come from each country's historical, social, and cultural background.

- We need a channel of communication such as the Bright Internet Global Summit (BIGS).
- We need an international body of collaborative research and deriving agreement such as Bright Internet Global Organization (BIGO).
- Two countries may agree at commonly acceptable level first, and continue talks.

5. Suggestion of Staged Implementation of IPP

❑ **First step:** Trust building through information exchange for crime prevention
Second step: Common Response to cyberattacks,
Establishment of responsible state behavior



6. Conclusion and the Future work

- **Further development of the Internet requires a secure cyberspace.**
  - **IPP is applicable as a preventive security framework for global cyber norm.**
  - China and USA share many similarities in implementing the IPP.
    . They are required to establish international cybersecurity norm.
    . Necessity of cybersecurity for economy, national security …
    . Sense of duty to establish it, as a bloc leader

- **Suggestion of** Staged implementation of **Internet Peace Principles**

- A composition and operation of international organization and conference as well as policy review for BI and IPP will be a main theme of discussion in the future.