Developments of International Norms on Cybersecurity

June 2018

Prof. Nohyoung Park
Korea Univ. Law School

Talk Points

- A Break-down of the UNGGE Process?
- Positive Movements for the International Law-Making for Cyberspace
- Three Major Players for International Law-Making for Digital Trade
- A Need for an Integrative Approach
- Conclusion

A Break-down of the UNGGE Process?

- After the continuing success of the UNGGE process, the 5th UNGGE failed to adopt a report by consensus in 2017.
  - The 3rd UNGGE recommended that "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment". (Para. 19)
  - The 4th UNGGE recommended 11 norms for the responsible behaviour of States. (Para. 13)

A Break-down of the UNGGE Process?

- After the continuing successes of the UNGGE process, the 5th UNGGE failed to adopt a report by consensus in 2017.
  - Negotiations among governmental experts in the 5th UNGGE were ultimately frustrated so as to prevent agreement on the application of international law to cyberspace. (Owen Bowcott, Dispute along cold war lines led to collapse of UN cyberwarfare talks, THE GUARDIAN (Aug. 23, 2017), https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges)
    - ✓ U.S. expert to the GGE argued that the GGE was misguided in not seriously considering the inclusion of the member states' right to self-defense against foreign-state attacks. (Michele Markoff, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, U.S. MISSION TO THE U.N. (June 23, 2017), https://usun.state.gov/remarks/7880). Michele Markoff argued that the recognition of the right to self-defense in the cyber context would "help reduce the risk of conflict by creating stable expectations of how states may and may not respond to cyber incidents they face."
    - ✓ Cuba, backed by China and Russia, opposed recognizing a right to self-defense, arguing that such a regime would "convert cyberspace into a theater of military operations and . . . legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs." (Declaration by Miguel Rodriguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017), http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.)

A Break-down of the UNGGE Process?

- What did not the 5th UNGGE achieve?
  - The 25 governmental experts were roughly successful to agree in the other areas such as norms of behavior, confidence building measures and capacity building measures.
  - They failed, however, in agreeing to how international law applies to cyberspace.
    - ✓ The western States tried to fix the explicit wording on the rules of self-defense, international humanitarian law and countermeasures in particular as the former two rules were agreed roughly in a diplomatic way in the 4th UNGGE.
    - ✓ China and Russia and some others thought that the recognition of those rules would make cyberspace militarized.

A Break-down of the UNGGE Process?

- What has the international society achieved nevertheless?
  - Since the 3rd UNGGE agreed to the applicability of international law to cyberspace, the groups of major States like G7 and G20, bilaterally and regionally as well as the UN General Assembly have confirmed the applicability of international law to cyberspace.
  - Even China and Russia would invoke their right to self-defense or countermeasures as found in Article 51 of the UN Charter and in the Draft Articles of State Responsibility and related international customary law respectively if they are victim to cyberattacks reaching to the level of "armed attack" or international wrongful acts of other States.
  - Thus, it would not be wise to simply state that cyberspace appears likely to remain an international "Wild West".

A Break-down of the UNGGE Process?

- It seems that States capable of conducting significant aggressive or malicious cyber operations do not want their capabilities to be regulated.
  - Those States may not really care about the collateral damage to civilians they would cause.
- Although States would not agree to or negotiate how to apply those international law rules to cyberspace especially between big powers and even in the UN generally, non-governmental experts have been successful in exercising the application of international law, for example with the publication of the two Tallinn Manuals.
  - The Tallinn Manuals are important in the developments of the application of international law to cyberspace, or international cyber law in that they showed the applicability of international law in peacetime as well as in armed conflicts while showing the problematic areas which must be tackled by States themselves.

Positive Movements for the International Law-Making for Digital Trade

- States, those same States, are fortunately moving towards making international law rules for cyberspace especially in the area of digital trade.
  - As the world economy is increasingly digital, so is trade.
    - ✓ The data flows crossing State borders, i.e., cross-border data flows are becoming more important in a global economy context, as data moves easily in and through cyberspace or the internet.
  - There is a good need for cross-border data flows to be governed under international law.
    - ✓ "Fragmented national rules on data, consumer protection, and the availability of online information can act as a major impediment to trade – creating new market barriers and pushing up costs." (WTO business focus group of the ICC)
    - ✓ A proliferation of different domestic e-commerce and digital trade provisions would create uncertainty for cross-border data flows.
    - ✓ Fortunately States are becoming interested in formulating the international rules for cross-border data flows both within and outside the WTO.

Positive Movements for the International Law-Making for Digital Trade

- The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), replacing the TPP signed by 12 Asia-Pacific States on 3 February 2016 and withdrawn by the US on 23 January 2017, has a good number of provisions relating to cross-border data flows in its Electronic Commerce chapter.
  - The CPTPP's rules on digital trade shows a model as they provide the rules on data protection and cybersecurity cooperation as well as those on trade in data.

Positive Movements for the International Law-Making for Digital Trade

- 71 WTO members adopted the Joint Statement on Electronic Commerce at the 11th Ministerial Conference on 13 December 2017. (WT/MIN(17)/60)
  - The MC 11, held in Argentine in December 2017, was not successful in launching multilateral negotiations to address e-commerce/digital trade in the WTO.
    - ✓ India in particular, who proposed discussion of data in the 5th UNGGE, opposed moving ahead on this initiative by stating: "When we do not know how and what future e-technology will develop and what regulation it will need, the question of freeing up regulation in this area should not even arise at this juncture."
    - ✓ A group of African countries also advocated staying within the WTO's current exploratory work program on e-commerce having been conducted and since 1998.
  - The US intends to use the discussions in the WTO as a valuable forum to develop commercially meaningful rules that address restrictions on digital trade, and will work with like-minded WTO Members who share the Administration's interest in moving forward on digital trade issues within the WTO. (USTR 2017 Annual Report, I-32)

Positive Movements for the International Law-Making for Digital Trade

- 71 WTO members adopted the Joint Statement on Electronic Commerce at the 11th Ministerial Conference on 13 December 2017. (WT/MIN(17)/60)
  - The 71 Members group agreed to initiate exploratory work toward future WTO negotiations on trade-related aspects of electronic commerce.
    - ✓Australia, Canada, the EU, Japan, Korea, Russia and the US were in the group, while China was not.
    - ✓The group held its first meeting on 14 March 2018.

Three Major Players for International Law-Making for Digital Trade

- The EU and the US share a broadly similar vision on digital trade, as shown in their 2011 trade-related ICT principles.
  - The US has a first mover advantage with IT industries and seeks to exploit this advantage at maximum.
  - The EU, having lost the lead to the US, has implemented the Digital Single Market (DSM) strategy.
    - ✓ The GDPR, a new data protection law with its expanded extraterritorial application, may make the EU the regulatory champion for cross-border data flows.
- China, while playing catch-up, has a numbers advantage and is exploiting that advantage based on the State-sponsored development of its high-technologies to become G2.
  - China has legitimate incentives to restrict access to its own data for any reasons.

Three Major Players for International Law-Making for Digital Trade

- China is unilaterally aggressive by enacting the Cybersecurity Law (CSL), effective on 1 June 2017, which is the most important domestic legislation for cross-border data flows.
  - Physical data must be stored in China;
  - There are mandatory security inspections of equipment prior to installation; and
  - There is mandatory law enforcement assistance and data retention regulations.
- There was a big concern about trade restrictive effects of the CSL raised in the meetings of the TBT Committee and the Council for Trade in Services of the WTO in 2017.

Three Major Players for International Law-Making for Digital Trade

- China also declared to advocate 'formulating cyberspace trade rules and effective policy coordination among countries' in its International Strategy of Cooperation on Cyberspace published on 1 March 2017.
- One of the strategic goals of China's participation in international cyberspace cooperation is to 'promote global development of the digital economy'.
  - China said that it "supports fair and open international trade, opposes trade barriers and trade protectionism and pursues an open and secure environment for the digital economy, to ensure the Internet serves the economy and innovation".
- China believes that "security guarantees development and development enhances security."
  - China said that "A healthy and strong digital economy would not be possible if the pursuit of absolute security is allowed to constrain momentum, openness or innovation, or necessary security regulation is not observed with the excuse of free market and free trade."

Three Major Players for International Law-Making for Digital Trade

- The US suggested a rather detailed positions on the rules for digital trade and free flows of information in particular on 12 April 2018 (JOB/GC/178):
  - Cross-Border Transfer of Data: "Trade rules can ensure that both consumers and companies are able to move data across borders without arbitrary or discriminatory restrictions."
  - Preventing Data Localization: "Trade rules can ensure that companies are not required to build or employ unique, capital-intensive digital infrastructure in every jurisdiction they serve, allowing them to better serve their customers."
  - Prohibiting Web Blocking: "Trade rules, including rules ensuring access to networks, can ensure that governments do not arbitrarily block or filter online content, nor require Internet intermediaries to do so."

A Need for an Integrative Approach

- Cybersecurity should be on the equal footing as data protection and digital trade, as the latter would not be successful without the former.
- A need to integrate the rules for the three areas is found in the digital trade rules of the electronic commerce chapter of the CPTPP, which cover the rules of the three areas of digital trade, data protection and cybersecurity cooperation.
  - Cross-border data flows are not restricted in principle. (Arts. 14.11 and 14.13)
  - Data protection for users of electronic commerce should be provided in accordance with the parties' domestic system. (Art. 14.8)
  - The importance of the cooperation on cybersecurity is recognized. (Art. 14.16)

A Need for an Integrative Approach

- There must be a good balance between a need to promote and protect cybersecurity, data privacy and digital trade, but there may be differences on how to keep a good balance depending on different States.
  - For example, there is a big concern in the US on the creation of probably unnecessary barriers to trade by the GDPR of the EU.
  - As to the relationship b/w cybersecurity and digital trade, both China and the US seem to agree that "security guarantees development and development enhances security" with the following differences:
    - ✓ China seems to favour more security by stating that "A healthy and strong digital economy would not be possible if the pursuit of absolute security is allowed to constrain momentum, openness or innovation, or necessary security regulation is not observed with the excuse of free market and free trade." (2017 International Strategy)
    - ✓ The US seems to be wary of more security by stating that "While cybersecurity threats undermine confidence in digital trade, overbroad efforts to protect cybersecurity can stifle the digital economy and even reduce security." (Communication, JOB/GC/178)
    - ✓ The US seems to believe that it's not responsible to stop innovation and progress through too much regulation.

Conclusion

- It would be unreasonable to state that there is no international law for cyberspace.
  - International law for cyberspace should be clarified although the applicability of international law to cyberspace in principle agreed internationally.
  - There are still gaps between big powers in agreeing to how certain international law rules apply to cyberspace.
  - Tallinn Manuals show the real applicability of international law to cyberspace while they show the problematic areas in the application of international law to cyberspace.
- There is a good move towards making international law for digital trade through FTAs as well as in the WTO.
  - Like in the areas of general international law, however, big powers would be very difficult to agree to the rules as they are directly related to cybersecurity.
- States are moving towards making international law rules relating to cybersecurity in specific areas like digital trade.