Hayashi, Koichiro

Conference Paper

Three Models for Sharing Cybersecurity Incident Information: A Legal and Political Analysis

14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Hayashi, Koichiro (2017) : Three Models for Sharing Cybersecurity Incident Information: A Legal and Political Analysis, 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/168485

Paper submitted to ITS Kyoto 2017

Three Models for Sharing Cybersecurity Incident Information : A Legal and Political Analysis

Koichiro Hayashi, Ph.D., LL.D. [1] [2]

Abstract

Though the international laws are applicable not only to the real world but also to cyberspace, the Internet is vulnerable against cyber attack, because it is fairly difficult to identify the real actor, when the attack is made by 'bots' or through anonymization methods (attribution problem). As the early Internet took for granted that the research community can maintain self-governance easily, concept of security-by-design is lacking. Hence the offenders have advantages over defenders, and the only effective measure for the defenders is the sharing of cybersecurity incident information, in order to analyze the characteristics of attack, and prepare for the next one. There are three types of sharing mechanism in the world; USA, EU, and UK models. This paper compares these models, and tries to extract some lessons for the future as well as for the other countries or areas. The most important factors for choosing the proper model are aggregated comparative advantages of defense, police, intelligence, and IT- related industry powers of the State concerned.

1. Cybersecurity in the international politics and 'attribution problem'

Cybersecurity is now one of the top priority issues in the international politics, as the Internet develops so rapidly and widely that our everyday life is dependent on the cyber infrastructure. The risk would be more serious, if the Internet of Things (IoT) became popular and the robots, drones, and the autonomous cars were common-place.

In this context, the summit meeting between then-President Obama of USA and President Xi Jinping of China in September 2015 may be a watershed event, for an agreement is unexpectedly announced that both States will never steal trade secrets by

[1] Professor of Law and Economics, Institute of Information Security, and Member of the Cybersecurity Strategy Headquarters, Cabinet Secretariat of Japan.

[2] The views expressed in this paper are those of the author, and do not necessarily represent those of the organizations, which the author is affiliated with..

using cyber attack (neither execute nor support). This is symbolic in two ways; first, it is the first time the world top leaders argued and agreed on cyber issues, which had never been an agenda for leaders but only for professionals. Second, what is more impressive is that both states recognized that the existing international laws are applicable not only to the real world but also to cyber activities.

However, attributing cyber activities to a specific person or an entity has long been near impossible, which prevented the enforceability of international laws. Meanwhile, United States continued to work very hard to identify the real actors beyond reasonable doubt. Two examples showed its capabilities; one was a prosecution of five military officers in Unit 61389 of the Third Department of the Chinese People's Liberation Army (PLA) for helping cyber attack to American corporations (U. S. Department of Justice [2014]). Another was a public announcement that North Korea is doubtful if it compromised Sony Pictures Entertainment's server and stole copies of then-unreleased films, trade secrets as well as bulk customer data. USA has not resolved 'attribution problem' completely, because North Korea denies any responsibilities, but USA must have a confidence in its capability of revealing attribution (Sanger and Perlroth [2014]).

This is actually a significant progress in global politics, and reflected in the interpretation of international laws. The International Group of Experts (IGE), headed by Professor Schmitt, made a remarkable effort to edit and publish 'Tallinn Manual on the International Law applicable to Cyber Warfare' in 2013 (Schmitt [2013], hereinafter Manual 1.0) and 'Tallinn Manual 2.0 on the International Law applicable to Cyber Operations' (Schmitt [2017], Manual 2.0).

Indeed, the international law is not well-organized and codified as the national law, but these manuals are now recognized as the most comprehensive and reliable restatements or commentaries of the existing international laws (including the customary laws) as far as cyber issues are concerned, though neither Russia nor China were represented in the drafting process.

In Manual 1.0, 'attribution' was treated as very difficult not to say impossible. The following old rules in Manual 1.0 represented IGE's point of view and its background feeling at that time. Especially Old Rule 7 indicated the difficulty of attribution.

Old Rule 5 – Control of cyber infrastructure: A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States,

Old Rule 6 – Legal responsibility of States: A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of

an international obligation.

Old Rule 7 – Cyber operations launched from governmental cyber infrastructure; The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation.

Four years later in Manual 2.0, above-mentioned Old Rules 5 and 6 are essentially maintained and strengthened by New Rules 6 and 7, and Old Rule 7 is replaced and expanded into New Rules 14 - 30 (More exactly, the essence of Old Rule 7 is absorbed in Comment 13 to New Rule 15 with minor changes.). The following rules and comments are the most symbolic ones.

New Rule 6 – Due Diligence (General Principle): A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.

New Rule 7 - Compliance with the due diligence principle: The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.

New Rule 14 - International wrongful cyber acts: A State bears responsibility for a cyber-related act that is attributable to the State and constitutes a breach of an international legal obligation.

New Comment 11 to Section 1 chapeau. (One sentence is omitted.) To illustrate, the Experts were of the view that as a general matter the graver the underlying breach (including considerations as to the primary norm concerned), the greater the confidence ought to be in the evidence relied upon by a State considering response. This is because the robustness of permissible self-help responses (such as retorsion, countermeasures, a plea of necessity, and self-defence) grows commensurately with the seriousness of a breach. However, they likewise agreed that the severity of the cyber operations directed at the injured State is a relevant consideration. For instance, a State facing low-level cyber operations that are merely disruptive may be in a position to accumulate more evidence for attribution than would a State suffering devastating cyber operations and needing to respond immediately to terminate them. Ultimately, the reasonableness of *ex ante* attribution must be assessed on a case-by-case basis, considering the

aforementioned, and other relevant, factors.

New Comment 14 to Section 1 chapeau. (Only the last sentence is shown.) Note that failure of the territorial State to take appropriate measures to control the individuals and cyber infrastructure may raise the issue of due diligence (Rules 6 - 7). In such a case, the State from which the operation are mounted may be responsible on its own accord for its failure to take the requisite remedial measures, rather than through attribution of the offending cyber operations.

The major differences between Manual 1.0 and 2.0 are two-fold; First, the applicability of the former was limited to cyber warfare, while the latter can be applied regardless of warfare or not. Second, there is a remarkable change as for the practice of attribution during the four years, and the editor as well as the experts is becoming more confident about the capabilities of searching and identifying the real actors, thus problem of attribution is fairly relaxed.

Moreover, New Comment 14 to Section 1 chapeau symbolizes the big mental change between the two Manuals, since it seems to convert the burden of proof from the defenders to the offenders (Please compare it with Old Rule 7.). Of course, it is not an easy task. The state that has a plenty of money and skilled manpower can only have a possibility. However, it is also true that attribution is not a one-or-zero type of clear-cut action. Usually, attribution is a function of possibilities and only incremental approach is feasible, as Rid and Buchanan [2015] properly pointed out.

> . On an operational level, attribution is a nuanced process, not a simple problem. That process of attribution is not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades. As a result, it is also a team sport — successful attribution requires more skills and resources than any single mind can offer. Optimising outcomes requires careful management and organisational process.

2. Self-defense and its lawfulness

Before discussing this topic, it is necessary to define several pivotal concepts, such as cyber activity, cyber attack, hack back, and so on. These concepts are often used by case-by-case implications, but the Manual 2.0 defines the basic notion for each word as follows (Glossary and Rule 92 in Schmitt [2017]).

Cyber activity: Any activity that involves the use of cyber infrastructure or employ

cyber means to affect the operation of such infrastructure. Such activities include, but are not limited to, cyber operation.

Cyber operation: The employment of cyber capabilities to achieve objectives in or through cyberspace. In the Manual, this term is generally used in an operational context.

Active cyber defence: The taking of proactive defence measures outside the defended cyber infrastructure. A 'hack-back' is a type of active cyber defence.

Hack-back: A type of 'active cyber defence', the main purpose of which is to take action against an identified source of a malicious cyber operation. Typically, a hack-back is desigened to mitigate the effects o, or stop, the malicious activity, or to gather technical evidence that can be used for attribution purposes.

Cyber attack: A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. (Rule 92, later cited again)

Those concepts must be interpreted subject to the prohibition of 'use of force' and 'armed attack', under the United Nations regime. And it is also important that self-defense, either individual or collective, is not prohibited until the Security Council takes necessary action. The UN Charter stipulates as follows.

Article 2 of the United Nations Charter

4. All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

Article 51 of the United Nations Charter

Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

These provisions were enacted just after the Second World War, and when the whole international community was in search of a long-standing peace. Therefore, the rules

are clear-cut, but fairly optimistic. The reality of the world politics is not such bright, and the armed conflicts are inevitable.

Facing with these severe realities, commentators of the Charter have an opinion that there exists a "force gap" between 'use of force' and 'armed attack'. In other words, while 'use of force' is limited to 'the military use of force', 'armed attack' is more strictly interpreted as 'the most serious and dangerous form of the illegal use of force (General Assembly Resolution on the Definition of Aggression (UNGA Res.3314, 14 Dec. 1874)), or 'the most grave form of the use of force' as ICJ (International Court of Justice) judged in Nicaragua v. US in 1986, because 'armed attack' is a precondition to resort to self-defense.

According to this definition, there is a wide grey zone, where 'armed attack' is prohibited but countermeasures, which is less serious but still a kind of 'use of force', is allowed. The next chapter discusses this point.

3. Countermeasures and their lawfulness

While Manual 2.0 describes more than twenty provisions regarding State responsibilities, it also provides a few on the countermeasures. The most essential principles are shown below (The only provision describing necessity in the same chapter is omitted to prioritize simplicity over comprehensiveness.).

New Rule 20 – Countermeasures (general principle) : A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State.

New Rule 21 - Purpose of countermeasures: Countermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with legal obligations it owes an injured State.

New Rule 22 – Limitation on countermeasures: Countermeasures, whether cyber in nature or not, may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate a peremptory norm. A State taking countermeasures must fulfill its obligations with respect to diplomatic and consular inviolability.

New Rule 23 – Proportionality of countermeasures: Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond.

New Rule 24 – State entitled to take countermeasures: Only an injured State may engage in countermeasures, whether cyber in nature or not.

New Rule 25 – Effect of countermeasures on third parties: A countermeasure, whether

cyber in nature or not, that violates a legal obligations owed to a third State or other party is prohibited.

The Manual 2.0 does not define what the countermeasures are, but in the world politics, measures such as CNE (Computer Network Exploitation) or EI (Equipment Interference) are common strategies, which the advanced States will take as a daily operation.

Computer Network Operations (CNO) has a broad meanings, covering both military and non-military operations, but in the US military term it consists of three activities, namely computer network attack, computer network defense, and computer network exploitation (Joint Pub. 3013) .

Computer Network Attack (CNA): Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.

Computer Network Defense (CND): Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.

Computer Network Exploitation (CNE): Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

While CNO is frequently referred to in the Unites States mostly in terms of military operation, Equipment Interference (EI) is used in the United Kingdom, mainly focusing on the investigatory powers for intelligence activities. Depending on the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA 2000), which is now being replaced by a new Investigatory Powers Act 2016 (IPA 2016), EI means the following (Equipment Interference, Code of Practice 2016).

Any interference (whether remotely or otherwise) by the Intelligence Services, or persons acting on their behalf or in their support, with equipment producing electromagnetic, acoustic and other emissions, or information derived from or related to such equipment, which is to be authorised under section 5 of the 1994 Act, in order to do any or all of the following:

(a) obtain information from the equipment in pursuit of intelligence requirements;

(b) obtain information concerning the ownership, nature and use of the equipment with a view to meeting intelligence requirements;

(c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);

(d) enable and facilitate surveillance activity by means of the equipment.

"Information" may include communications content, and communications data as described in section 21 of RIPA 2000.

According to above-mentioned definition, CNA may go beyond the limit of countermeasures, while both CNE and EI seem to remain within the limit. However, it is still ambiguous whether there is a clear distinction between CNA (or cyber attack) and CNE (EI, or cyber espionage). There are two contrastive views; one is represented by a famous security architect Bruce Schneier, and the other is by Thomas Rid, professor of political economy at King's College London.

Schneier [2014] insists as follows;

> Cyber-espionage is a form of cyber-attack. It's an offensive action. It violates the sovereignty of another country, and we're doing it with far too little consideration of its diplomatic and geopolitical costs. The problem is that, from the point of view of the object of an attack, CNE and CNA look the same as each other, except for the end result.
>
> The offensive military operations in cyberspace, be they CNE or CNA, should be the purview of the military. In the U.S., that's Cyber Command. Such operations should be recognized as offensive military actions, and should be approved at the highest levels of the executive branch, and be subject to the same international law standards that govern acts of war in the offline world.
>
> If we're going to attack another country's electronic infrastructure, we should treat it like any other attack on a foreign country. It's no longer just espionage, it's a cyber-attack.

On the contrary, Rid takes the opposite position and published a paper with provocative title 'Cyber War Will Not Take Place' (Rid [2011]). After examining the realities of four preceding cyber attacks (Siberian pipeline explosion in 1982, an attack on Estonia in 2007, cyber attacks on Georgia in 2008, and Stuxnet in 2010), he concludes.

So far, there is no known act of cyber war, when war is properly defined. ----------
All politically motivated cyber attacks are merely sophisticated version of three activities that are as old as warfare itself; sabotage, espionage, and subversion.

His point of view is consistent with majority opinion of the international law experts, since Manual 2.0 prescribes as follows.

Rule 92 – Definition of cyber attack: A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to person or damage or destruction to objects.
Comment 2 to this article: The notion of 'attack' is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilians and civilian objects may not be 'attacked' (Rule 92, 94, and 99).This rule sets forth a definition of 'attack' that draws on that found in Article 49(1) of Additional Protocol 1: attacks means acts of violence against the adversary, whether in offence or defence', By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military operation. Non-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks.

However, the differences between Schneier and Rid may not be so wide as the first impression indicates. For, Schneier as a computer engineer, emphasizes the difficulty of distinguishing between 'cyber attack' and 'cyber espionage', while paying less attention to the strict legal definition of these terms. On the contrary, Rid as a scholar in international politics, is keen to the definition of law, while paying less attention to engineering issues. Probably both are recognizing the ambiguities of the notions concerned, and focus on their expertise.

In the middle, there is a view that the action is 'kinetic' or not is a reasonable 'Merkmal' to judge whether it is 'armed attack' or not. However, I will refrain from going into the details, since this paper is not a textbook of international laws but focuses on how to share cybersecurity incident information.

4. Asymmetries between offense and defense

Unfortunately the Internet is vulnerable against cyber attack, because it is fairly difficult to identify the real actor (attribution problem), when the attack is made by 'bots' or through anonymization. Although anonymity can be revealed by technology, it is a kind of pike and shield competition, which takes a huge amount of time and

money to reach a satisfactory level of detection. Hence, only the state with rich money and expertise can afford.

As the early Internet took for granted that the research community can maintain self-governance easily, concept of security-by-design, where ID (Identification) is the first step, is lacking. Anonymity can be realized by encryption technologies and applications such as TOR (The Onion Router) or Command & Control server, which can dictate the taken-over server to act as a proxy. So anonymity is directly linked with difficulty of identifying the real actor.

Anonymity usually causes stealthiness. For example, penetrated virus can stay in the network without being detected, and even the owner of the taken-over PC does not always notice (e.g. Trojan Horse). Anonymity also leads to escalation, where mischief, accidental event, bad act can be easily escalated to tort and/or criminal conduct, and more into use of force and/or attack (for example, once targeted on critical infrastructure).

These conditions lead to a general tendency that the offenders have advantages over defenders. Rid [2011] recognizes these discussions.

> Conventional wisdom holds that cyberspace turns offense/defense balance on its head by making attacking easier and more cost-effective while making defending harder and more resource-intense. Cyber attack, the standard argument goes, increased the attacker's opportunities and amount of damage to be done while decreasing the risks (sending special code is easier than sending special forces).

Indeed, Rid challenges the traditional wisdom in the following discussions, but it is generally believed that there are seven aspects of asymmetries, of which offenders always have comparative advantages (see also Chart 1).:

1) Even the single point breakthrough will be congratulated as a success on offenders' side, whereas the entire defense is required for defenders.
2) Offenders can take advantage of any easy-to-get tools regardless of legal or illegal, but defenders are limited to lawful measures.
3) Offenders are not formally organized but act as guerrillas with agility and flexibility, while defenders are forced to respond domain-by-domain as regular army, which sometimes lacks timely action.
4) Offenders recruit many volunteers and reserves with small amount of money, while defenders depend upon formal soldier recruitment and educate cyber-professionals within the organization.

5) Offenders are scattered around the world but maintain loose cooperation among similar organizations (e.g. Anonymous). On the other hand, defenders are mainly domestic organizations, and global cooperation is not common.
6) Some states support offenders' action implicitly, but defenders must observe the international rule.
7) Offenders utilize any computer power including taken-over servers and PCs, thus the computer power is infinite. To the contrary, defenders have to use the limited resource with secure environment.

Chart 1 : Asymmetries between Offense and Defense

Item	Offense	Defense
Success or failure	One-point breakthrough deemed successful	100 % defense required
Attack/Protect tool	Easy to get	Difficult to find
Combatant	Quasi-state organization or outlaw guerrilla	Formally-organized soldier
Potential combatant	Many volunteers	Limited within the formal troops
International Cooperation	Loosely-united members (cf. Anonymous)	Basically domestic corps
Underground cooperation	Underground cooperation suspected	Within the International legal regime
Power and control	Distributed computer power utilized by command and control server	Limited resource under the secure environment

1

In order to compensate for the disadvantages, the defenders are forced to take multi-layer defense, which takes defensive measures as much as and as widely as possible. Network security, system security, device security, firewall, anti-virus software, physical security, human resource management, preparedness against social engineering, incident response, and so on, are put together and used as multi-layer defense.

5. Information sharing: the only effective measure against cyber attack

As the development of encryption technology as well as command-and control system via the zombie PCs (bot net), it is becoming difficult to identify the actual wrong doers, which generates both 'attribution' problems and asymmetries mentioned above. In order to overcome these disadvantages, the only effective measure for the defenders is the

sharing of cybersecurity incident information, to analyze the characteristics of attack, and prepare for the next one. Therefore defenders are eager to gather and/or share as much information as possible.

This trend is popular among developed economies, but there are subtle differences due to comparative advantages as well as security cultures of the state concerned. Today the most remarkable examples are USA, EU, and UK models. We will compare these models in detail.

5.1 USA model

USA has enacted Cybersecurity Act of 2015, of which the most important part is called Cybersecurity Information Sharing Act (CISA), where the sharing of incident information is made possible depending on the following premise.

1) As both the government and large corporations are capable of dealing with cyber incidents by themselves, the policy role is limited to facilitating the collaboration among players.
2) As USA is a typical litigation society, the first priority for the corporations is to exempt them from liabilities (especially anti-trust liability and disclosure via Freedom of Information Act = FOIA) caused by information-sharing.
3) On top of the above-mentioned institutions, government is ready to share the classified information with a corporation, staffed with a security-cleared employee.
4) Sharing information is supposed to be either Cyber Threat Indicator (CTI) or Defensive Measures (DM).

For nearly two decades, potential cyber threats information has been shared through industry-specific Information Sharing and Analysis Centers ("ISACs"), established in 1998. However, participants of ISACs have expressed concern that perceived risks associated with information sharing—including potential civil liability, antitrust issues, and the protection of intellectual property and other proprietary business information—have limited the effectiveness of ISACs and other information-sharing.

CISA provided the safe harbors from liability for private entities that share cybersecurity information in accordance with specified procedures, and it also authorized various entities, including outside the federal government, to monitor their information systems and operate defensive measures for cybersecurity purposes.

Simultaneously, President Obama signed Executive Order to open the National Cybersecurity and Communications Integration Center (NCCIC), a civilian agency in the Department of Homeland Security (DHS), tasked with coordinating the sharing of information within the federal government and with private entities and state, tribal,

and local government agencies (collectively, "Non-Federal Entities"). It also added DHS to the list of federal agencies that approve classified information-sharing arrangements to streamline private companies' ability to access classified cybersecurity threat information.

Among many briefing papers on CISA, the most excellent summary is Sullivan and Cromwell [2015], which describes the following as the most important parts of the legislation:

> **Sharing centralized in DHS.** After a long tug-of-war between DHS and the intelligence community, DHS—and specifically NCCIC—has been selected as the primary gateway for cybersecurity information sharing between the private sector and the federal government. DHS is required to set up an automated system to forward information it receives to many other federal entities, including the Department of Defense and the Office of the Director of National Intelligence, in real-time or as quickly as operationally practicable.
>
> **Liability protections require sharing "in accordance" with CISA.** To benefit from CISA's safe harbor from civil liability, private entities' sharing activity must be "conducted in accordance" with CISA's provisions. Entities that share information should keep clear records evidencing their compliance with CISA to ensure they can benefit from its liability protections.
>
> **Broad safe harbors from liability.** Once triggered, CISA's safe harbors from liability are broad. Private entities sharing information are generally shielded from civil, regulatory, and antitrust liability based on their sharing. CISA does not expressly exclude instances of either gross negligence or willful misconduct from its liability protections. Sharing cyber threat indicators and defensive measures with the federal government will also not constitute a waiver of any privilege or protection provided by law, and shared information is exempt from disclosure under freedom of information laws. Information shared with the federal government will remain the commercial, financial, or proprietary information of the originating Non-Federal Entity only if that entity so designates it.
>
> **Requirement to remove information known to be unrelated personal information.** One of CISA's requirements is that Non-Federal Entities review information to be shared, or utilize a technical capability, to remove any information that the Non-Federal Entity "knows at the time of sharing" to be personal or personally identifying information not directly related to a cybersecurity threat.
>
> **Communications with regulatory authorities permitted.** Though the availability of

liability protection turns on using the DHS process, regulated entities can continue to communicate directly with their respective federal regulatory authorities regarding cybersecurity threats without losing CISA's liability protections.

Limited use of shared information by federal and state governments. The permissible purposes for which shared information may be used by federal and state governments are circumscribed. Privacy and civil liberty advocates have raised concerns in particular regarding the potential breadth of CISA's authorization for governments to use shared information to respond to, prevent, mitigate, investigate, or prosecute a specific (though not necessarily imminent) "threat of serious economic harm."

No duty to share. CISA does not create any duty to share cyber threat indicators or defensive measures and expressly prohibits the federal government from attempting to coerce sharing by withholding cybersecurity information or other benefits such as government contracts, addressing concerns some privacy advocates had expressed that companies could be forced to turn over large swaths of user data to the government.

No creation of a duty to warn or act. CISA does not impose a duty to warn or act based on the receipt of shared information, but it does not expressly shield entities from liability in the event of a good-faith failure to act. An entity that receives information about a cybersecurity threat to its networks may remain subject to claims premised on common law causes of action such as negligence if it fails to respond diligently.

Authorization to use defensive measures. CISA also authorizes private entities to use defensive measures for cybersecurity purposes on an entity's own information systems and on the information systems of other consenting entities.

As for the last point, the report draws attention to the fact that the measures such as 'destroy, render unusable, provide unauthorized access to, or substantially harm to third-party information systems' are excluded from the definition of " defensive measures". And as such, 'CISA does not authorize "hacking back," which generally remains illegal pursuant to the Computer Fraud and Abuse Act and guidance published by the Department of Justice'. These comments are consistent with the majority opinion of the international law experts as mentioned above.

It is also notable that USA seems to become more reluctant than before to collect communications data in bulk. This attitude is apparent in the Privacy Shield agreement

between USA and EU. The EU-US Privacy Shield is a replacement for the International Safe Harbor Privacy Principles, which were declared invalid by the European Court of Justice in October 2015, saying that Safe Harbor does not qualify as ‘adequate levels of protection’ prescribed in the Article 25(6) of Data Protection Directive (95/46/EC).

Soon after this decision, the European Commission and the U.S. Government started talks about a new framework and in February 2016 they reached a political agreement. The European Commission published a draft “adequacy decision”, declaring principles to be equivalent to the protections offered by EU law. One of its purposes is to enable US companies to more easily receive personal data from EU entities under the reciprocal treatment between the two.

On the launch of EU-US Privacy Shield, EU Press Release emphasized the following points (EU Commission [2016c]).

> **Strong obligations on companies handling data:** under the new arrangement, the U.S. Department of Commerce will conduct regular updates and reviews of participating companies, to ensure that companies follow the rules they submitted themselves to. If companies do not comply in practice they face sanctions and removal from the list. The tightening of conditions for the onward transfers of data to third parties will guarantee the same level of protection in case of a transfer from a Privacy Shield company.
>
> **Clear safeguards and transparency obligations on U.S. government access:** The US has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear limitations, safeguards and oversight mechanisms. Everyone in the EU will, also for the first time, benefit from redress mechanisms in this area. The U.S. has ruled out indiscriminate mass surveillance on personal data transferred to the US under the EU-U.S. Privacy Shield arrangement. The Office of the Director of National Intelligence further clarified that bulk collection of data could only be used under specific preconditions and needs to be as targeted and focused as possible. It details the safeguards in place for the use of data under such exceptional circumstances. The U.S. Secretary of State has established a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism within the Department of State.
>
> **Effective protection of individual rights:** Any citizen who considers that their data has been misused under the Privacy Shield scheme will benefit from several accessible and affordable dispute resolution mechanisms. Ideally, the complaint

will be resolved by the company itself, or free of charge. Alternative Dispute resolution (ADR) solutions will be offered. Individuals can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism. Redress possibility in the area of national security for EU citizens' will be handled by an Ombudsperson independent from the US intelligence services.

Annual joint review mechanism: the mechanism will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available and will issue a public report to the European Parliament and the Council.

Among the four points listed above, the most important factor in relation to the topic of this paper is treatment of bulk data, since privacy advocates expressed the strongest concern about it. Actually, pressure from EU side might be so strong that USA stepped back from the previous position, and promised to refrain from collecting personal data as a bulk with a little exception for national security. However, it is still uncertain whether this attitude will be maintained under Trump administration.

5.2 EU model

EU issued Directive on Security of Network and Information Systems (NIS Directive、Directive 2016/1148) in July 2016, and it entered into force in August 2016. EU is handicapped in two ways compared to US; First there are 28 member states, which are different in size, budget, demography, and especially IT capability. And second, EU does not have enough competitiveness in ICT industry. Therefore, the first target of this directive is to set a bottom-line (minimum harmonization in Article 3) for cybersecurity .

As a bottom line, NIS Directive lays down specific obligations for Member State (MSs) to adopt a national NIS strategy, to designate National Competent Authorities (NCA), Single Points of Contact (SPoC) and specific NIS tasks to Computer Security Incident Response Teams (CSIRTs).

In addition, the Directive orders to designate Operator of Essential Service (OES) and

Digital Service Provider (DSP), which are obliged to report the serious incidents without delay to the government concerned respectively. Otherwise, they will be fined. MSs will have 21 months to transpose the Directive into their national laws and 6 months more to identify OES and DSP

An Operator of Essential Service (OES) is a public or private entity, which provides an essential service for the maintenance of critical societal and/or economic activities, depends on network and information systems, and for which an impact on these systems would produce "significant disruptive effects" on its ability to provide its service. OES includes banking, energy, transport, financial market infrastructure, health, drinking water, digital infrastructure (Articles 4 (4), 5 (2), and Annex Ⅱ).

A Digital Service means a service offered at a distance by electronic means at the request of an individual recipient of services (Article 4(5), Annex Ⅲ, and Article 1 (1) b of Directive 2015-1535), but specified in this Directive as either of the three categories of Online Marketplaces, Online Search Engines or Cloud Computing Services.

Some sectors are already regulated or may be regulated in the future by sector-specific EU laws. Whenever those acts impose requirements, their provisions will take precedence over the corresponding provisions of the NIS Directive, so long as they are equivalent in effect.

Chart 2 below is from Deloitte [2015], which summarizes and compares the obligations imposed on OES and DSP. Judging from the wide and detailed obligations, it seems to be an EU way to expect OES and DSP pioneering the cybersecurity field.

Chart 2 ; Security requirements for OES and DSP

Security requirements	OES	DSP
A. Take technical and organizational measures to manage the risks posed to the security of network and information systems	Yes	Yes (partially)
B. Provide information needed to assess the security of network and information systems, including security policies.	Yes	Yes
C. Provide evidence of effective implementation of security policies, such as the results of security audits.	Yes	No
D. Execute binding instructions received by the NCA to remedy their operations.	Yes	No
E. Remedy any failure to fulfill the requirements set out in the NIS Directive.	No	Yes
F. Designate a representative in the EU when not established in the EU, but offering services within the EU.	No	Yes

Cybersecurity is directly linked with EU's policy under the banner of 'Digital Single Market,' and the key objectives of the Commission in the field of cybersecurity are described as follows (EU Commission [2016b]).

> Increasing cybersecurity capabilities and cooperation:
> The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level. In this area, the Directive on security of network and information systems (the NIS Directive) is the main instrument supporting Europe's cyber resilience.

In order to pursue these goals, the Commission will propose how to enhance cross-border cooperation in case of a major cyber-incident. Given the speed with which the cybersecurity landscape is evolving, the Commission will also bring forward its evaluation of the European Union Agency for Network and Information Security (ENISA), which will possibly lead to the adoption of a new mandate.

Actually prior to the formal announcement of the Directive, ENISA published its position in a briefing paper, and showed its readiness to implementation (ENISA [2016]).

> As a result of the work it has carried out in the past, ENISA is ideally positioned to assist the Member States in implementing the NIS Directive once it is adopted. This note has provided a number of arguments explaining how this can be achieved in practice for specific requirements raised by the Directive.

Indeed, the effort by ENISA in cybersecurity field is widely recognized, but the total competitiveness of EU in terms of ICT industries is doubtful, since there are few EU-born corporations in the designated three field of DSP (Online Marketplaces, Online Search Engines or Cloud Computing Services). Especially the search engine market is dominated by Google. Therefore, NIS Directive has a special provision on the jurisdiction regarding DSP as follows.

Article 18 Jurisdiction and territoriality

1. For the purpose of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A

digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.

2. A digital service provider that is not established in the Union, but offers service referred to in Annex Ⅲ within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member State where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.
3. The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.

These provisions reveal that EU are afraid of Google and other competitors circumventing EU's jurisdiction, but at the same time that EU must pay attention to these corporations, since there is a contrastive difference of treatment between OES and DSP (As for OES, there is no provisions comparable to Article 18.).

5.3 UK model

In November 2016, the UK Investigatory Powers Bill received royal assent and passed into law as the Investigatory Powers Act (IPA) 2016 (hereinafter, IPA 2016, or simply the Act). The Act builds on the work of three independent reviews undertaken during 2015 and aims to do three things ; 1) consolidate the powers already available to UK law enforcement, security and intelligence agencies to obtain the content of, and data about communications, 2) overhaul the mechanism for authorizing and overseeing these powers, and 3) ensure that the powers afforded in existing legislation are fit for the digital age.

IPA 2016 has been controversial throughout its passage through Parliament due to the far-reaching powers it hands to government agencies to require technology and communications businesses. Privacy advocates nicknamed it as 'Snoopers' Charter', but the House of Commons supported the Bill with wide margin of 444 to 69 vote.

Actually powers in the Act include all technological measures, which Edward Snowden revealed and condemned, namely interception, acquisition of communications data (CD), equipment interference, three kinds of Notice (Retention Notice, National Security Notice, and Technical Capability Notice). Moreover, powers also include not only targeted acquisition but bulk acquisition of data, although the latter are permitted only for the intelligence agencies under 'double lock' scrutiny (Warrant issued by the Ministry of State must be approved by the Judiciary Commissioner.).

In a press release, the Home Office has stated that some provisions of the Act will not be in place for some time as they require "extensive testing". The Home Office is reportedly developing plans for implementing these provisions including Code of Practice (CoP) and will set out a timetable in due course. It further stated that such a timetable will be subject to detailed consultation with industry and operational partners, without indicating who such partners might be.

It is necessary to learn and analyze what kind of powers are permitted under what kind of conditions before we judge the real value of IPA 2016, in the circumstances where the opinions are clearly divided. So I will analyze these matters one by one, of which I will focus on the differences of terms and conditions between targeted and bulk acquisition of data, because the strongest concern surrounds bulk data.

First regarding interception, the traditional way of acquiring communications content, the differences are summarized as the following three points. 1) Bulk interception is allowed only for the intelligence with special operational purpose, while targeted interception is also available for law enforcement. 2) In relation to this reason, bulk interceptions covers overseas communications only (either sender or recipient is located overseas), while targeted interception is allowed both for overseas and domestic communications. 3) Both interception require 'double lock', but there is an exception of 'emergency' in case of targeted interception. Bulk interception is strictly scrutinized without this exception. (See also Chart 3 where three points are shown in red characters.)

Chart 3 : Targeted Interception and Bulk Interception

	Targeted	Bulk
Applicable communications	Domestic and overseas	Overseas (either caller or receiver)
Applicant	Law enforcement and intelligence agencies	Intelligence agencies only
Warrant issuer	Minister of State, Scottish ministers	Same as the left column
Reason	1) National security, 2) serious crime, 3) economic well-being related to 1)	Reason 1)~3) of the left column plus 'specified operational purpose'
Double lock	Ex ante approval by judiciary commissioner, except emergency (ex post approval admitted)	Ex ante approval by judiciary commissioner without emergency exception
Expiration term	6 months + 30 days for each renewal	Same as the left column

Second as for acquisition of communications data (CD) and/or Internet connection record (ICR), four major differences can be pointed out. 1) Bulk acquisition is allowed only for the intelligence with special operational purpose, while targeted acquisition is also available for law enforcement. 2) Applicant and reasons for targeted acquisition are fairly broad, while bulk acquisition is narrowly tailored. 3) There is a clear difference on warrant requirement: it is required only for bulk, not for targeted acquisition. In the latter, authorization by the senior officials of the applicant office replaces the warrant. 4) Double lock is necessary only when the information comes under 'privileged' one in case of targeted acquisition, but in case of bulk it must be strictly observed. Again these points are shown in Chart 4, and the major differences are indicated in red characters.

Chart 4 : Targeted and Bulk Acquisition of Communications Data (CD) and Internet Connections Record (ICR) as well

	Targeted CD (or ICR)	Bulk CD (or ICR)
Applicable communications	Domestic with extra-territoriality exception	Overseas(either caller or receiver)
Applicant	Law enforcement, intelligence, and local agencies	Intelligence agencies only
Warrant issuer	No warrant. only authorization by senior official of the applicant required	Minister of State
Reason	10 reasons, including 1) National security, 2) serious crime, 3) economic well-being related to 1)	Reason 1)~3) of the left column plus 'specified operational purpose'
Double lock	Only in case of privileged information, approval by judiciary commissioner required. In case of local government, additional authorization required	Ex ante approval by judiciary commissioner without emergency exception
Expiration term	1 month + 1 month for each renewal	6 months + 30 days for each renewal

Third, the differences between targeted and bulk Equipment Interference (EI) is almost same as in case of interception except 'double lock'. 1) Bulk EI is allowed only for the intelligence with special operational purpose, while targeted EI is also available for law enforcement. 2) In relation to this reason, bulk EI covers overseas communications only (either sender or recipient is located overseas), while targeted EI is allowed both for overseas and domestic communications. 3) Both EI require 'double lock', and there is no exception for 'emergency'. (See again Chart 5 where three points are shown in red

characters).

Chart 5 ; Targeted Equipment Interference (EI) and Bulk EI

	Targeted	Bulk
Applicable communications	Domestic and overseas	Overseas(either caller or receiver)
Applicant	Intelligence, defense intelligence, and law enforcement agencies listed in Schedule 6	Intelligence agencies only
Warrant issuer	Minister of State, Scottish Ministers, and Director of law enforcement agencies	Minister of state
Reason	1) National security, 2) serious crime, 3) economic well-being related to 1)	Reason 1)~3) of the left column plus 'specified operational purpose'
Double lock	Ex ante approval by judiciary commissioner, except emergency (ex post approval admitted)	Same as the left column
Expiration term	6 months + 30 days for each renewal	Same as the left column

By the way, some people, especially who are working for Internet-related business or privacy advocates, are keen to the inclusion of ICR and express the strong concern about it. A few media follow the same way. Their concern is half correct and half wrong. Indeed, it is probably the first time that Internet-related data are treated at the same level with voice telephony record. But it is natural and reasonable, because the present telecommunications traffic is transmitted via the Internet rather than the traditional network. Therefore, they are wrong.

IPA2016 imposes data retention (by Data Retention Notice = DRN) and access obligations on 'over-the-top' service providers (OTTs), such as providers of messaging and other applications, and expands the current obligations that affect traditional telecoms companies (Communications Service Providers = CSPs) under existing legislation. As far as CSPs and OTTs are treated equally, their concern is not reasonable.

However once DRN is issued, communications data must be retained for a maximum period of 12 months (plus 30 days extension for each renewal) for access by law enforcement agencies, and other public bodies, without a warrant. This system is unique among developed economies, and whether warrantless access is permissible invites a controversy. In this regard, their concern is correct. I will return to this point in the next chapter.

More problem exist about encryption removal: Both CSPs and OTTs may, when served with a notice (Technical Capability Notice =TCN), be required to remove any applied encryption to assist in giving effect to interception warrants. Privacy advocates are concerned about the possibility of regulations being passed which impose obligations relating to the removal of electronic protection (i.e., encryption) applied by technology providers. This actually happened in USA, where Apple was requested to help FBI in decryption but it refused to obey.

Anyway, it is not deniable that the most remarkable characteristics of UK model rests on the power of bulk data while USA is now slightly changing its policy after EU-US Privacy Shield agreement. Why does UK stick to bulk data? Probably there are four reasons. First, UK intelligence communities used to rely on 'content' of communications rather than communications data (CD). However, as the terrorist widened their communications tools and so-called 'home-grown' terrorists increase, they are asked to find a covert relationship among the untargeted potential actors, which is impossible without huge bulk data.

Second, as encryption becomes popular, the needs for decryption also increase, which is only possible by analyzing bulk data. Third, It is becoming technically feasible to gather bulk data by tapping in the submarine cable, and analyze them in near-real time. And fourth, there is 'a culture of secrecy' (or a culture of confidentiality) in UK, that makes it acceptable to install the world densiest distribution of CCTV (Closed Circuit TeleVision) around the country to monitor and detect the wrong-dowers.

Of course, the more dependence on bulk data is usually accompanied by the more risk of information leakage. Therefore, the Act pays much attention to establish a strict procedure to gather and use bulk data in such a way that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the interception is to acquire intelligence relating to individuals outside the UK, even where the conduct occurs within the UK. Similarly, interference with the privacy of persons in the UK will be permitted only to the extent that it is necessary for that purpose.

Before closing this sub-chapter, it is necessary to briefly touch upon the influence of ECJ's decision which declared DRIPA invalid. On Dec. 21, 2016, the European Court of Justice (ECJ) ruled that the UK's Data Retention and Investigatory Powers Act (DRIPA) 2014, which expires on 31 December 2016, was unlawful because it allowed for the general and indiscriminate retention of EU citizens' data. The ruling could be problematic for the Investigatory Powers Act 2016, which replaces DRIPA and largely replicates the contested laws in question.

This decision includes various points to be discussed both legally and politically; first

from legal viewpoint, there is a complexity of jurisdictions between European Convention on Human Rights (over which European Court of Human Rights = ECtHR has jurisdiction), and EU Charter of Fundamental Rights (over which European Court of Justice = ECJ presides). And the former is expected to remain effective for UK even after Britain's exit from EU (Brexit). Second from political side, it is the most delicate timing to discuss the issue, because the negotiations of Brexit is just to begin, and the future cooperation in the field of intelligence is supposed to be one of the covert agenda.

Presumably, Mr. Anderson's opinion represents the moderate viewpoint, who is the most cited person when it comes to terrorism or investigatory powers (House of Commons [2017).

> We could do what we liked with data collection in this country if we had no interest in getting our hands on the personal data of the Europeans. If we took that autarchic line and said, "We are not interested in anything you send and we are just jolly well going to do things our own way", then we could do it untrammeled by the European Court. I am saying that, if we want records of various kinds for various purposes, be they financial, travel records or whatever, then even our domestic powers of collection are going to come under scrutiny, much as they are under scrutiny at the moment.

6. Some implications

So far, we have been examining the characteristics of USA, EU, and UK models respectively, but now it is time to compare three models and extract some implications. It is natural that each country or area has its own comparative advantages and concentrates its ability on the advantageous points. Therefore, we compare their comparative advantages and disadvantages. Please read the following sentences while referring to Chart 6 and 7 frequently.

USA has so strong competence in military (defense), ICT-related industry (or in so-called 'military-industrial complex'), and intelligence that its cyber strategy, especial sharing of incident information, is to let either of them go its own way, and the role of government is limited to eliminating the obstacles which prevent sharing and cooperation. It is a new development that NCCIC is established and expected to play a role of coordinator between government and Non-Federal Entities, but the power of military as well as intelligence will not decline (Actually, some functions of intelligence such as COMINT by NSA are reserved within the military). According to Lowenthal [2009], 75~80% of intelligence activities in USA are under the influence of Department

of Defense (DoD) in terms of either strategy, budget or personnel. The similar will be true for cyber activities. We may call this model as 'public-private equal sharing' model.

On the contrary, EU is in the contrastive position. It has a police power, but lacks its own military and intelligence functions, although the power of some MSs are enough beyond the average Thus it has to start with information sharing from scratch. The bottom line is to ask Member State to secure the last resort, such as the national security policy, NCA, SPoC, and CSIRTs. Ir also depends heavily on OES and DSP, and imposes the same obligations on foreign operators as far as it has the main office or the representative within the EU territory. This model may be called as 'initial step for integrated sharing'.

UK's response to cyber-attack is different both from US and EU models, since it is more government-centered approach. UK has a long history of intelligence, and continues to depend more on data gathering than sharing. IPA 2016 covers 1) targeted interception of communications, 2) bulk interception, 3) retention of communications data, 4) acquisition of such data, 5) bulk acquisition, 6) targeted equipment interference, and 7) bulk equipment interference. Surprisingly, almost all communications intelligence (COMINT) activities are covered and rationalized under the new 'double lock' (Judiciary Commissioner system). Of course, there is a strong private actor such as British Telecom, but in general it may be called 'government-led sharing'.

The followings are minimal implications derived from three models; 1) Every state has her own history and culture. Therefore, there will be no single answer to cope with cyber security. 2) However, the experiences in other countries are informative to any state, and deserve attention. 3) Existing three examples are to be studied carefully, and some parts of them will be applicable to other states or regions. 4) Scarcity of resource such as budget, capable workforce, and experience, will be the most critical determinant to choose the model suited to each state. 5) For the handicapped states, it is clever to collaborate with advanced states, instead of doing everything by themselves.

In order to test the applicability of above-mentioned analyses, I have tried to recommend an appropriate model for Japan and inserted it in Chart 6 and 7, which belongs to 'private initiative guided by government' model. The most urgent task for Japan is to establish a united CERT (Computer Emergency Response Team) or CSIRTs (Computer Security Incident Response Teams). because the responsibilities are divided among GSOC (Government Security Operation Center), JP-CERT/CC (Japan-Computer Emergency Response Team/ Coordination Center for private entities), and ad hog organization responsible for Olympic/Paralympic 2020. As Japan is skillful in incremental approach, the last one will contribute to the future as a prototype.

Chart 6 : Comparative Advantages of State in Cybersecurity(CS)

◎= super strong, ○= strong, △= average, × = weak

Comparative advantage	USA	EU	UK	Japan
Defense	◎	×	○	△
Police	△	○	○	○
Intelligence	○	×	◎	×
IT-related industry	◎	△	△	△ (except telecom.)
National CS center except military operation	NCCIC(national CS and Communications integration Center), under DHS	No single org., but retained for each Member state	NCSC(National CS Center) as an entity within GCHQ	No integration center except GSOC at NISC , JPCERT/CC, and ad hoc org. for 2020 Olympic
Note	Tacitly supported by NSA?	Some State may be stronger than the average .	Long-standing security culture	

Chart 7 : Models for Incident Information Sharing

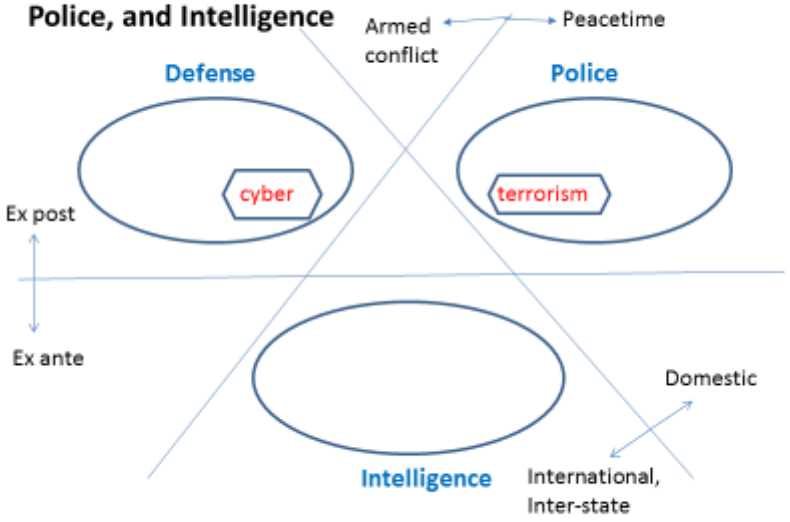
Method	USA	EU	UK	Japan
Tentative name for the Model	Public-private equal sharing	Initial step for integrated sharing	Government-led sharing	Private initiative guided by government
Information to be shared, or reported	CTI(Cyber Threat Indicator and DM(Defensive Measures)	Incident report to government, mandatory for OoES(Operator of Essential Service) and DSP(Digital Service Provider)	GCHQ gathers and analyzes huge amount of info., and ready to share with private org., if necessary	Government pushes sharing mechanism, but operation is voluntary.
Conditions	Private corps. required security clearance, if ask for classified info.	OoES and DSP required to report incident info. to the single point of contact (SPoC), then shared with other Member States	GCHQ can gather and analyze bulk data, following the procedure of IPA 2016.	Secrecy of communications are most strictly observed in the world.
Role of government	Equal partner	Play a role of liaison for inter-state cooperation.	Superior provider of info.	Fairly weak due to limited capability

7. Short comments for the future

Although it is useful to learn lessons from the past experiences of other states, it neither excludes nor decreases the need for thinking about the ideal model toward the future. The world is so rapidly changing that today's optimizations does not necessarily guarantee the future effectiveness.

Here, the traditional demarcation among defense, police, and intelligence functions, each of which is responsible for 'national security' respectively and as a whole, is to become obsolete. Instead, convergence and cooperation among the different functions are remarkable in the following five points. 1) Defense is primarily responsible for 'armed attack', but cyber attack blurs the boundary between wartime and peacetime. 2) Who should treat terrorism needs a new approach, because they are globalized (beyond national territories) and equipped with heavy weapons. 3) The combination of cyber and terrorism creates more complexity. 4) Intelligence is believed to be controlled by the

Figure 1 : Traditional demarcation among Defense, Police, and Intelligence



division of powers between foreign and domestic (counter-intelligence), HUMINT and SIGINT and so on, but cyber espionage requires new method. 5) In general, ex post' response becomes ineffective, but 'ex ante' dealing invites a great concern against violation of human rights. (See Figure 1.).

It is not an easy task to predict the future, and Figure 2. is just a primitive trial, where two points are to be noted. First, the driving force to require the change is the power of cyber and terrorism. Once these two activities are neatly combined, it is

difficult to confront. Second, it is a natural way to strengthen each function respectively. Therefore in the defense, 'cyber' is included as the fourth domain, but still 'war against terrorism' is controversial, since 'war' must be carefully defined and treated. In the police, counter terrorism becomes both domestic and international issues, thus cooperation in the global perspective is inevitable. In intelligence field, its role will be more crucial and it will be a must, because cyber and/or terrorism is stealthy.

Figure 2 : Convergence of Defense, Police, and Intelligence Activities against Terrorism with Cyber powers

However, to give up the traditional demarcation will be accompanied by loss of the advantages, it maintained for a long time. Above all, the negative effect on human rights including privacy seems most serious. If I take USA as an example, there was a clear demarcation between defense and police such as Posse Comitatus Act of 1978, though its main purpose is a reconciliation of North v. South just after the Civil War. Also there was a contrastive difference regarding the way of interception of communications between ECPA (Electronic Communications Privacy Act of 1986) and FISA (Foreign Intelligence Surveillance Act of 1978), of which the conditions are more severe in the former than in the latter. These traditions are of themselves worth attention, and we have to establish a new appropriate system to have a right balance between the conflicting values.

Anyway, I will again emphasize that each state had better select its own way of treating cyber issues, depending on its culture and history. However in that process, it is wise to learn lessons from other countries and pay attention not only to the

contemporary comparison but projections to the future, since there is no royal road, as all intelligence textbooks tell us.

Acknowledgement

I am grateful to the members of ad hoc study group for 'the bulk data under IPA 2016', and especially to Mr. Yoshihiro Tagawa, who led the group, for useful insights and comments. I also thank the anonymous reviewers of this paper for their suggestions to improve the quality. Though these two group's contribution is highly appreciated, the final responsibility for the content of this paper is attributable to the author alone.

References

Deloitte [2015] 'Agreement reached on EU NIS Directive'
https://www2.deloitte.com/lu/en/pages/risk/articles/agreement-new-eu-network-information-security-directive.html

ENISA [2016] 'ENISA's Position on the NIS Directive'
https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-position-on-the-nis-directive

EU Commission [2016a] 'The Directive on Security of Network and Information Systems (NIS Security Directive)'
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

EU Commission [2016b] 'Cybersecurity in Digital Single Market'
https://ec.europa.eu/digital-single-market/en/cybersecurity

EU Commission [2016c] "European Commission launches EU-U.S. `Privacy Shield: stronger protection for transatlantic data flows' (Press Release)
http://europa.eu/rapid/press-release_IP-16-2461_en.htm

Nakatani, Kazuhiro [2015] 'Cyber Attack and International Law', "Journal of International Law" Vol.3 (in Japanese)

House of Commons [2017] "Brexit: implications for national security" Briefing Paper No.CBP7798, 31, March 2017

Hayashi, Koichiro [2016a] 'Melancholy of Cybersecurity Practitioners', "Yobou Jihou", The General Insurance Association of Japan (in Japanese)

Hayashi, Koichiro [2016b] 'How to Share Cybersecurity Incident Information', "Journal of JSICR", Vol. 34, No. 3 (in Japanese)

Lowenthal, Mark M. [2009] "Intelligence: From Secrets to Policy (4th Edition)", CQ Press

Rid, Thomas [2012] 'Cyber War Will Not Take Place', "Journal of Strategic Studies", Vol. 35, Issue 1

Rid, Thomas and Ben Buchanan [2015] 'Attributing Cyber Attacks', "Journal of Strategic Studies", Vol. 38, Issue 1-2

Sanger, David and Nicole Perlroth [2014] 'U.S. Links North Korea to Sony Hacking, "The Now York Times, December 17, 2014

Schmit, Michael N. (ed.) [2013] "Tallinn Manual on the International Law applicable to Cyber Warfare", Cambridge University Press

Schmitt, Michael N.(ed.) [2017] "Tallinn Manual 2.0 on the International Law applicable to Cyber Operations", Cambridge University Press Michael N. Schmitt [2013] International Law applicable Cambridge University Press Cambridge University Press

Schneier, Bruce [2014] 'Computer Network Exploitation vs. Computer Network Attack' https://www.schneier.com/blog/archives/2014/03/computer_networ.html

Sullivan and Cromwell [2015] 'The Cybersecurity Act of 2015', Dec.22, 2015 https://www.sullcrom.com/.../SC_Publication_The_Cybersecurity_A...

UK : Investigatory Powers Bill 2015-16 to 2016-17 http://services.parliament.uk/bills/2015-16/investigatorypowers.html

US : Cybersecurity Act of 2015 as Division N in the Consolidated Appropriations Act of 2016 https://www.justsecurity.org/.../2015/.../Cybersecurity-Act-of-2015

U.S. Department of Justice Press Release [2014] 'U. S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', May 19, 2014 https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor