G-SEC WORKING PAPER No. 33

How EU and Japan Deal with the Challenges of Cybersecurity in the eGovernment Domain in the Emerging Age of IoT?

Carmen Elena CIRNU[1]

February 2016

Abstract

This paper represents the foundation of a future extended research that aims to investigate more in depth how cybersecurity shall evolve in the e-government domain considering the challenges represented by the emerging IoT (Internet of Things). The present paper addresses the question to be investigated and presents the general and specific framework of cybersecurity, critical infrastructures policy and regulation, e-government and e-services domain. With the EU trying to implement cross-border services using digital service infrastructures and Japan fostering its government sector, questions related to cybersecurity and cyberdefense policies for this sector represents emerging subjects. What this paper is suggesting and intend to develop in a future research is the need to declare the e-government sector and particularly the digital service infrastructures as critical infrastructures and to further propose a dedicated cybersecurity policy and specific measures designated to ensure a safe and secure space for adoption and use of e-services, since boostering the use of e-services would represent a benefit for the economy.

[1] Guest Research Fellow, Global Security Institute (G-SEC), Keio University. E-mail: carmen.cirnu@gmail.com.

1. Regulatory Environment for Cybersecurity in EU and Japan

At a glance, the objective of cybersecurity is to reduce the risk of cyber attacks, to minimize successful cybersecurity attacks and to build trust on the security of the Internet.

The EU economy is already affected by cybercrime activities against the private sector and individuals. Cybercriminals are using sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.

1.1. Cybersecurity Regulations in EU: EU Cybersecurity Strategy and EU International Cyberspace Policy

Cybersecurity policy-making as an emergent field is more and more a national policy priority with explicit strategies in several countries since the participation to any international cooperation or policy frameworks is related to cybersecurity performances of a state, explicitly because cyber-attacks are not constrained by administrative borders, but for the entire network system that is interconnected.

One of the core documents of the EU dealing with cybersecurity is the Digital Agenda. The document sees Internet trust and security as vital to a vibrant digital society, and sets out 14 actions to improve cybersecurity readiness. These actions include the establishment of a well-functioning network of CERTs (Computer Emergency Response Teams) at national level covering all of Europe; the organisation of cyber-incidents simulations and the support to EU-wide cybersecurity preparedness. Accordingly, the policy on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital ICT infrastructure by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities, both at national and at EU level.

The **EU Cybersecurity Strategy** was published in February 2013 as part of the commitment to an ‘open, safe and secure cyberspace’ along a proposal for a Directive concerning measures to ensure a high common level of network and information security across the European Union. These initiatives complement and are consistent with existing ones related to electronic communications and data protection regulatory frameworks, as well as to the protection of European critical infrastructure.

The Cybersecurity Strategy for the European Union and the Commission proposal for a Directive on Network and Information Security put forward legal measures and give incentives aiming at making the EU's online environment the most secure in the world. By strengthening preparedness, cross-border cooperation and information exchange, the proposed Directive would enable citizens to reap the full benefits the digital environment offers and it would allow the public and private sector to trust digital networks' services at

national and EU level. As network and information systems are globally interconnected, cybersecurity has a global dimension too, thus the strategy addresses international cooperation as a key priority.

The Strategy is accompanied by a legislative proposal to strengthen the security of the EU's information systems in order to encourage economic growth as confidence in buying online and using the internet grows. According to the document, the **priorities** for EU international cyberspace policy are defined as following:

- *Freedom and openness*: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace;

- *The EU's laws, norms and core values apply as much in cyberspace as in the physical world*: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments;

- *Developing cybersecurity capacity building*: the EU engages with international partners and organisations, the private sector and civil society to support global capacity building in third countries. This includes improving access to information and to an open internet, and preventing cyber threats; and

- *Fostering international cooperation in cyberspace*: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.

The **principles** adopted by the EU Cybersecurity Strategy:

- *Protecting fundamental rights, freedom of expression, personal data and privacy*: Any information sharing for the purposes of cybersecurity, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field;

- *Access for all*: Limited or no access to the Internet and digital illiteracy constitute a disadvantage to citizens. The Internet's integrity and security must be guaranteed to allow safe access for all;

- *Democratic and efficient multi-stakeholder governance*: The EU reaffirms the importance of all stakeholders in the current Internet governance model and supports this multi-stakeholder governance approach; and

- *A shared responsibility to ensure security*: All relevant actors, whether public authorities, the private sector or individual citizens, need to recognise this shared responsibility, take action to protect themselves and if necessary ensure a coordinated response to strengthen cybersecurity.

The EU vision presented in this strategy is articulated in **five strategic priorities**, which address the challenges highlighted above: achieving cyber resilience; drastically reducing cybercrime; developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP); develop the industrial and technological resources for cybersecurity; and establish a coherent international cyberspace policy for the European Union and promote core EU values.

Cyber incidents do not stop at borders in the interconnected digital economy and society. As different legal frameworks and jurisdictions may be involved, a key challenge for the EU is to clarify the roles and responsibilities of the many actors involved.

At EU level there is a certain difficulty to clearly distribute the roles related to cybersecurity among different levels of authority generated by the complexity of the field. There is a general approach to the need of promoting a holistic effort where stakeholders in different levels are included in order to ensure the security of the ICT infrastructure. The interoperability and cross-borderless of various ICT systems are facing challenges, more specifically in technical terms, standards need to be defined and implemented at national and European level to insure the interoperability.

Nevertheless local and regional authorities need to acknowledge their role in ensuring the protection of e-Governance systems working through: regional and/or local applications or platforms; real-time collection of data on cybercrime; and awareness and training initiatives for both civil servants and citizens. Given the complexity of the issue and the diverse range of actors involved, centralised, European supervision and national implementation may represent a solution. National governments shall organise the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks. At the same time, due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement. To address cybersecurity in a comprehensive way, activities should span across three key pillars: Network and Information Security (NIS), Law Enforcement, and Defence.

The EU Cybersecurity Strategy mentions that increasingly, more complex and no borders cybersecurity incidents requires a clear and effective approach in order to deal with the growing challenge of cyber attacks. It is clearly stated and the governments are aware that these incidents can cause major damage to safety and the economy, so efforts to prevent, cooperate and be more transparent about cyber incidents must improve since previous efforts by the European Commission and individual Member States have been too fragmented.

Among the proposed measures laid down by the mentioned document, it is stated that operators of critical infrastructures in some sectors (financial services, transport, energy, and health), enablers of information society services (notably: app stores e-commerce platforms, Internet payment, cloud computing, search engines, and social networks) and public

administrations must adopt risk management practices and report major security incidents on their core services.

Nevertheless the strategy does not clearly states what approach shall be made for protecting eGovernment domain, more specifically the digital service infrastructures. They involve dealing with sensitive data, so special measures shall be designated and implemented.

1.2. Cybersecurity Strategy in Japan

In September 2015, Japan released its national cybersecurity strategy, considering the cyberspace as an essential foundation of Japan's socio-economic activities that attracted a great deal of users due to its non-discriminatory and non-exclusive nature of easy accessibility.

Japan is very aware of the cyber "diastrophism" provoked by ICTs evolution even if it is only in its initial stage. The Strategy points that recently, all kinds of "things" or physical objects have begun to be connected to networks including the Internet. Along with the increasing connectivity, physical objects and people in real space have become interconnected in a multi-layered manner without physical constraints, by harnessing the free flow of information and accurate data communications in cyberspace. Due to such linkages, there is an emergence of an "interconnected and converged information society" where physical space and cyberspace have become highly integrated.

Since the cyberspace is vulnerable and malicious activities are increasing, **identifying the major threats and the response to those threats** are considered essential also due to the increasing dependency of socio-economic activities on cyberspace and the evolution of organized and highly sophisticated methods, or modus operandi, of cyber attacks that might be state-sponsored have caused grave damages and exerted negative impacts on the people's daily lives and socio-economic activities, and consequently, threats against national security have become more serious in the recent years.

Japan’s Strategy strengthens that, due to the arrival of the interconnected and converged information society, malicious activities in cyberspace will cause extensive impact on all kinds of connected physical objects and services, and the damage caused by cyber attacks will spread more rapidly and widely in physical space; therefore, **it is anticipated that the people's living will be exposed to more immense cyber threats in the future**.

Japan affirms the following **basic principles** in policy planning and implementation for reaching the objective of this strategy: assurance of the free flow of information; the rule of law; openness; autonomy; and collaboration among multi-stakeholders.

The following policy approaches have been established:

- *Improving socio-economic vitality and sustainable development*: With regard to the IoT systems for realizing new services in the interconnected and converged information society, enterprise management, and business environment supportive for them, the Government will take the following *strategic approaches*: creation of secures IoT systems, promotion of enterprise management with a security mindset, improvement of cybersecurity business environment;

- *Building a safe and secure society for the people* through: measures for the protection of the people and society, **measures for critical infrastructure protection and measures for the protection of the government bodies;**

- Ensuring peace and stability of the international community and national security through: ensuring national security (including protection of governmental bodies and social systems), maintaining peace and stability of the international community and cooperation and collaboration with countries around the world; and

- Cross-cutting approaches to cybersecurity through advancement of R&D, development and assurance of cybersecurity workforce.

Japan's Strategy seems to be more articulated on the domain investigated by this research paper. While EU is proposing mainly a general framework, Japan is making the steps toward more specific cyber defence policies related to our topic of interest.

2. Framework for Critical Infrastructures in EU and Japan

2.1. Critical Information Infrastructure Protection in EU

In May 2009 the Communication of Critical Information Infrastructure was released. Its aim was to protect European space from cyber disruptions by enhancing security and resilience, through five pillars: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; and criteria for European critical infrastructures in the field of ICT.

In June 2012, European Parliament gave a Resolution on "Critical Information Infrastructure Protection: towards global cyber-security." The main achievements of this CIIP policy are:

- The establishment of the European Forum for member states of the European Public-Private Partnership for Resilience;

- Carrying out of pan-European exercises; and

- Adoption by ENISA (European Union Agency for Network and Information Security) of a minimum set of baseline capabilities and services and related policy recommendations for CERTs to function effectively.

This document is briefly presented in this working paper and its scope within here is to point that digital service infrastructures (and no specifically e-government or e-service) are listed among the sectors considered critical infrastructures by the EU.

2.2. Measures for Critical Information Infrastructure Protection according to Japanese Cybersecurity Strategy

According to the Japanese CIIP Strategy, there are five main policies: maintenance and promotion of the safety principles; enhancement of information sharing system; enhancement of incident response capability; risk management; and enhancement of the basis for CIIP.

The social infrastructures designated to ensure people's living and economic activities, as well as a wide range of information systems has been used for the functions of these social infrastructures. In the circumstances, the public and private sectors must work together to protect CII, in particular, information and communications services, electric power supply services, and financial services, of which the functional failure or deterioration would risk enormous impacts to the people's living conditions and economic activities. As CII is required by its nature to provide a continuous supply of service, for its protection, it is crucial to reduce the occurrence of system failures caused by cyber attacks or other reasons to the minimum extent; it is also crucial to carry out early detection of any system failure and prompt recovery from damage or failure.

Among its proposed strategic actions, the CII documents states that for local governments, their responsibility and the cooperative measures taken by the Cybersecurity Strategic Headquarters to support them are prescribed under the Basic Act on Cybersecurity. **All local governments,** regardless of their scales, have a unique status, as they **are required to meet the security standards similar to those of the governmental bodies and government-related entities, because of their functions, e.g. handling sensitive information.** There is an environmental transition expected in local governments, for they will need to adopt new systems due to the nationwide introduction of the *My Number system*. The Government will provide necessary assistance, in accordance with the Basic Act on Cybersecurity, for their security assurance, and will examine and take necessary measures regarding the information systems of local governments, with the object of strengthening cybersecurity for the operation of the My Number system.

At the same time, the Government is expected to take necessary cybersecurity measures, based on consideration of effective approaches, including:

- Operational systems development and improved operational frameworks build upon advanced cybersecurity measures;

- Separation of the systems for handling the affairs using the individual numbers prescribed under the *Act on the Use of Numbers to Identify a Specific Individual* in the Administrative

Procedure from the Internet;

- Enhance monitoring and oversight mechanisms based on professional and technical knowledge and experiences, in coordination with relevant entities;

- Build frameworks with capabilities of monitoring and prompt detection of cybersecurity incidents, taking account of possible information sharing with the Government Security Operation Coordination team (GSOC); and

- Work to improve environments necessary to make the best balance between increased user-friendliness and security assurance (specifically with regard to the intergovernmental and public - private coordination for authentication at the occasion of introducing the My Number system).

The governmental bodies have the mission to defend and support the people's living and socio-economic activities, therefore the shutdown of their functions is a significant concern to the national security. The execution of missions of the governmental bodies relies on CII and other services provided by business operators responsible for social systems. The document states that in this context, Japan and business operators in charge of CII and other social systems will further enhance their daily efforts to bring, share, and analyze beneficial information, such as vulnerabilities and attack information, and address to threats in a necessary manner. It is also expected to accelerate interactive information exchange between the public and private sectors.

3. eGovernment Domain in EU and Japan: Overview of Services

eGovernment is affected by the development and changes of the web, with increasing focus on the Government 2.0 paradigm. It concentrates more on the demand side, on user empowerment and engagement, as well as on benefits and impacts that address specific societal challenges, rather than simply providing administrative services online (ex. eSENS: electronic Simple European Networked Services Pilot Project). From silo and government centricity toward becoming more user centric and user driven, users and other legitimate stakeholders are being invited more openly into a participative and empowering relationship with government in relation to service design and delivery, the working and arrangements of the public sector and public governance more widely, as well as public policy and decision making.

Stages of the e-government correlated to stages of the web:

- Web 1.0: webpages and websites, e-mail, instant messaging, SMS, simple online discussion, etc.;

- Web 2.0: allows users to provide and manipulate content and get directly involved. Web 2.0 sites typically have an “architecture of participation” that encourages users to add value to

their application as they use it, for example through social media dialogue around user-generated content in a virtual community;

- Web 3.0: evolution toward wide-scale ubiquitous seamless networks (grid computing), networked and distributed computing, open ID, open semantic web, large-scale distributed databases and artificial intelligence; and,

- Web 4.0: global semantic web: according to Tim Barners-Lee we are on the verge of the age of semantic web that exploits the internet of data rather than the internet of documents we now have. This will enable intelligent users of the Internet like asking questions rather than simple searching for keywords and more automatic data exchanges between databases, data mining and similar uses.

3.1. eGovernment, eServices and EU Digital Service Infrastructures in Europe

eGovernment and eServices

The term of eGovernment was introduced in late 1980 in Europe and formally conceptualized in 1993 by the US Government. eServices represents a branche of the eGovernment and it represents a highly generic term, usually referring to the provision of services via the Internet (the prefix “e” standing for “electronic”), thus e-Service may also include e-Commerce, although it may also include non-commercial services (online), which is usually provided by the government.

As Jeong (2007) explains eService constitutes the online services available on the Internet, whereby a valid transaction of buying and selling (procurement) is possible, as opposed to the traditional websites, whereby only descriptive information are available, and no online transaction is made possible.

Connecting Europe through digital bridges to the benefit of citizens, businesses and public administrations

EU is aiming to implement cross-border digital public services in order to remove digital barriers to citizens' and businesses' mobility in the Single Market so they can access eGovernment services abroad as easily as from home.

Even at this moment the cross border delivery of online government services is considered too limited in Europe. A 2011 survey on barriers to the single market found that about half of the barriers could be solved if eGovernment were able to work across borders. The EC have launched Large Scale Pilot projects (LSPs) in key areas of online public services highly relevant to the Digital Single Market - such as eID (STORK), eProcurement (PEPPOL), eHealth (EPSOS), business mobility (SPOCS) and eJustice (eCODEX). These LSPs achieve interoperability between existing national IT systems in the different areas. The digital

service infrastructures of the Connecting Europe Facility (CEF) are in domains such as eGovernment, cybersecurity, eHealth or cultural heritage. They comprise "core service platforms" and "generic services" that are offered to businesses and citizens to achieve cross border solutions. All the eGovernment services are in areas of public interest such as eID, eSignature, eInvoicing, eProcurement, and business mobility, but are linked also to domain such as eHealth, hence requiring a good governance between all the relevant services.

The main component of a digital service infrastructure is the core service platform which is a central hub at EU level to which national infrastructures link up and thus create a link between different national infrastructures.

There are two types of DSIs (Digital Service Infrastructures):

- Building Block DSIs - this is the basic digital infrastructures intended to be re-used in other digital services. By re-using the BB (Building Block) DSIs the service provider will: reduce costs, shorten time to market, and facilitate interoperability. Examples of building block DSIs: eID & eSignature: services enabling cross-border recognition and validation of eIdentification and eSignature; eDelivery: services for the secured, traceable cross-border transmission of electronic documents; Automated Translation: services allowing pan-European digital services to operate in a multilingual environment; Cybersecurity: services to enhance the EU-wide capability for preparedness, information sharing, coordination and response to cyber threats; and eIvoicing: services enabling secure electronic exchange of invoices.

- **Sector Specific DSIs**: *eProcurement* (services enabling EU companies to respond to public procurement procedures from contracting entities in any member state); *eHealth* (services enabling cross-border interactions between citizens and health care providers as well as between the health care providers); other interoperable cross-border online services such as *eJustice*, *EESSI* (Electronic Exchange of Social Security Information), *Business Registry* (services to interconnect business registers in all MS to enable the exchange of information), *Business Mobility* (services to enable the handling of all administrative procedures for setting up and running a business in another EU country electronically through Points of Single Contact) and others. Sector Specific DSIs deliver more complex trans-European online services for citizens, business and public administrations within one specific policy area (such as health or justice for example). If relevant BB DSIs are available, they must be re-used in Sector-Specific DSIs.

The most comprehensive approach for this European vision regarding eServices is the pilot project e-SENS that embodies the idea of European Digital Market development through innovative ICT solutions. The project aims to consolidate, improve, and extend technical solutions to foster electronic interaction with public administrations across the EU. The project also aims to develop the digital infrastructure for improving the quality of public services in EU.

One gap that this working paper is raising is the lack of cybersecurity policies and procedures for those infrastructures. Dealing with highly sensitive data may need some procedure to include this domain on the list of critical infrastructures and to accordingly plan a strategy of cyber defence.

3.2. eGovernment in Japan: Services for Citizens

In Japan, the Government is working on promotion of initiatives such as online use of administrative procedures, electronic provision of government information, optimization of work and systems, improvement of government procurement related to information systems, and information security measures.

Japan released its latest IT Strategy in September 2015, focusing on three major pillars: eGovernment, Open Government and Open Data. This document is based on the "Basic Act on the Formation of an Advanced Information and Telecommunications Network Society" dated January 2001 and the documents and strategies that followed it (including the 2013 "Declaration to be World's Most Advanced IT Nation"). According to the document, the society that Japan should seek to become is: a society that encourages the creation of new and innovative industries and services and the growth of all industries; the world's safest and most disaster-resilient society where people can live safely, with peace of mind and comfort; and one-stop public services that anyone can access and use at any time.

The one-stop public services that anyone can access at any time and from anywhere shall implement several measures: to provision highly convenient electronic government services; to reform the government information systems at national and local level; and to reinforce IT governance in government.

Social Security and Tax Number System: Individual Number Card

Japanese government is implementing the social security and tax number system as a key element for economic growth. When introducing the Social Security and Tax Number System, various security management measures are taken in terms of both institution and computer system. For example, the basic management of personal data has not changed. The different governmental agencies are responsible for taking control over personal data management. The Social Security and Tax Number System does not mean that the data is centralized and controlled.

In addition, Individual Number Card (also known as My personal number) is currently under implementation. The Individual Number itself is not going to be used as a matching key among all concerning governmental agencies. When data transmission action among certain governmental agencies is taken place through the Cooperation Network System for Personal Information, the network system generates a different code for each agency and uses it as a coordination key, shutting out other administrative agencies. The necessary measures, such as

review and improvement of current guidelines, are continuously discussed to strengthen further security for achieving full utilization of Individual Number in Japan.

The adoption and use of Individual Number Card is encouraged also for local government offices, incorporated administrative agencies, national universities, and private sectors to utilize Individual Number Cards as their ID cards for staff members. In addition, it is considered to use Individual Number Cards as cash cards, debit cards, and credit cards, as well as to make the use of the Disclosure System of Personal Information Cooperation Record through ATMs starting in FY 2017.

As Japanese authorities are very aware that for such promotion, it is necessary to ensure the security of personal data and the prevention of financial crimes. As online confirmation system for health insurance qualification is developed shortly after July 2017, Individual Number Cards will be expected to be used as health insurance cards. Moreover, it will be also considered to unify Individual Number Cards with other governmental cards, such as seal impression registration identification cards. It will be gradually realized to add more functionalities based on the discussion about how far Individual Number Cards can take the role of public certification or permission confirmation of every kind.

Currently under discussion is the necessity to develop a technology to make the functionality of the public key infrastructure available on smartphone. The reading application format is planned to be developed in 2017 and in 2019, for downloading of user confirmation functions.

In fiscal year 2017, the Japanese government intends to expand one-stop services in the area of motor vehicle inspection and registration work. In order to realize that, it is concerned to utilize the public key infrastructure functions of Individual Number Cards as well as rationalization of document submission process.

The plans for the coming years are very ambitious as the public services provided by the Social Security and Tax Number System is intended to be diversified with the realization of certain public services available by using Individual Number Cards at convenience store. The scope of available public service by using Individual Number Cards in convenience store is to obtain copies of residence certificates, personal seal registration certificates, family register copies, and so on.

The Disclosure System of Personal Information Cooperation Record (planned to start in January 2017) will enhance the electronic public services sector. It aims to the submission of the public and the private certificates through use of electronic lockbox functions, and one-stop services for certain life events such as house-moving notice and obituary notice to be possible. It is also considered the service accessibility to such administrative procedure to be available with various kinds of digital devices, such as TV and smartphones.

In order to realize such environment, the government and the private sector need to strengthen their collaboration to develop the system with the positive use of the public key infrastructure functions of Individual Number Cards.

The institutional measures and its computer system development are considered further in depth in order for those who obtain delegation of authority from corporate representative to be able to handle application submission and contract exchange digitally without conducting face-to-face communication nor paper based documents. Based on the considered measures and its computer system, the entire governmental procurement from examine bid participation qualification to exchanging contract agreement will be gradually shifted to digitalization with promoting the use of Individual Number Card and Corporate Number. The first step of starting the system is targeted in Fiscal Year 2017.

It is intended that functions for the provision of services that were previously undertaken by government to be opened to the private sector and highly convenient services to be created through collaboration by the public and private sectors.

Open user environments that utilize cloud computing are being developed through the standardization and sharing of data format, terminologies, codes, and characters and the public release of application interfaces (API) to facilitate active participation by members of the public as stakeholders. With regard to the standardization and sharing of characters in particular, information systems developed in the future will in principle use character data platforms that conform to international standards. When designing online services, the objective will be to digitalize the entire service value chain with the aim of increasing convenience and raising overall efficiency. Marketing techniques will be employed for the design of user-centric services and services will be provided through appropriate channels such as smartphone and tablet terminals.

Efforts will be made based on “Policy for Improving Convenience of Online Procedures” (decided in a liaison committee of ministry CIOs [Chief Information Officers] on April 1, 2014) and “Action Plan for Development of Disclosed IT Utilization Environment in the Field of Administration” (decided in a liaison committee of ministry CIOs on April 25, 2014). With regard to government websites, measures will be taken pursuant to the “Basic Policy on the Provision and Promotion of Use of Government Information the a Websites and Other Means” (decided in a liaison committee of ministry CIOs on March 27, 2015) and websites will be updated to create sites that are more convenient from users’ perspectives by progressively publicly disclosing API for government websites and taking other measures.

In preparation for the utilization of cloud computing and the Social Security and Tax Number System, Japanese government intend to implement: operational reforms; security measures to properly manage important information including personal information, and highly convenient online services including the one-stop services that users want; customizable services that can be accessed via mobile terminals; and efficient administrative operations.

The implementation of the new e-government strategy is planned to lead also to comprehensive reforms in public administration investment in IT. When updating individual information systems, individual governmental ministries and agencies will adopt detailed reform plans that specify their vision for improving services and streamlining and raising the efficiency of operations, the details of necessary reforms to legal, organizational and operational systems, and the effects of investment. Operational and system reforms will be implemented systemically based on these plans.

In addition, extensive use of cloud computing will lead to higher efficiencies on larger scales, seamless collaboration that eliminates vertical organizational divisions, improved ability to respond rapidly and flexibly to change, and substantial cost reductions through more efficient administrative operations.

4. Challenges of Cybersecurity for eGovernment

Probably the biggest operational challenge to eGovernemnt is cybersecurity, including threats to identity, privacy and data systems. Adequate privacy and data protection are crucial for reaping the benefits of eGovernment. If they are in place and work well they can provide stable, predictable and confidence-building frameworks.

The shift toward a more open government has created threats as well as opportunities. A lot of malicious attempts to access public administration networks are seen and the rage of the attacks goes from recreational hackers to sophisticated cyber-criminals. Moving public sector information online has also direct and indirect ramification across the large canvas of e-government areas often not considered. According to some experts (Millard, 2011) for example, many governments are setting security systems too high for the functionalities deployed, resulting in a waste of resources that could have been used to shore up more vulnerable systems (for example, sophisticated PKI [Public Key Infrastructure] and digital signature systems when simple passwords or PIN [Personal Identification Number] code would suffice).

Challenges to cybersecurity may include unauthorized access to or use of data and public sector information (public sector managers need to be aware of these unintended consequences) and consequently fears of data insecurity tends to be the biggest impediment in the use of eGovernment.

As acknowledged also from the analysis of cybersecurity strategies presented above, cyber defence response is highly variable and central governments are much more likely to have measures in place than local government, but the whole public sector is facing operational independence among its various parts. This leads to a clear recommendation to align the strategies and the demands also to the central (European) governments and for the local ones.

Several key areas are under consideration when dealing with challenges related to cybersecurity in the eGovernment domain and this includes (according to Millard 2011)

privacy, trust, data security, loss of data control or human behavior. Those areas shall be taken into consideration when further analyzing the implementation of electronic public services in Europe or Japan.

Apart from Japan, EU intended to go in parallel with introducing (proposing, piloting, implementing) electronic public services (also cross-border), while Japan decided to go first for what EU calls “eID” and then based on it to implement several electronic public services.

What seems to lack to both approaches is a dedicated and more targeted measures to face the challenge of cyber threats.

5. Conclusions, Recommendations and Proposal for Future Research

Based on the documentation carried out in the last months, there can be several recommendations and proposal for future research. Several major domains shall be taken into consideration when dealing with cybersecurity recommendations in the public sector. First, a risk assessment and management process to secure and constantly improve the network and information systems shall be established followed by the enforcing of information security policy by means of obligations, sanctions as well as rights. Increasing perception of cybersecurity issues and improving digital literacy and skills in terms of recognition and management of threats shall be on the “short list” of actions. Also an important aspect is seeking support beyond the local/regional public administration to achieve economies of scale, effectiveness and piloting.

There is an important role that governments shall play in the area of internet security for broader adoptions and use of e-services but this importance is not yet sufficiently reflected in the limited cybersecurity-related initiatives described within literature or available on the web. Awareness of cyber-threats over digital infrastructures and by governments is not enough. Governments need to implement concrete actions to allow safer access to e-services to increasingly demanding citizens. Infrastructural solutions, common rules, standards and specifications need to be implemented.

Better protection against cyber-attacks requires, in the first instance, governments to be aware of the need to articulate effectives also national and transnational interaction mechanism, allowing access to external resources (e.g. cybersecurity research and development, tailored information, and certified training) and experiences (e.g. cooperation).

Additionally, governments are expected to actively interact with citizens on cybersecurity issues, allowing, for example, end-users’ reporting and feedback.

Assuming that digital service infrastructures (and consequently e-services) are declared critical infrastructures, the governments need to work on both awareness on cybersecurity needs and challenges, and preparedness. Information exchange platforms are crucial to the correct functioning of infrastructure and infrastructure services that rely on interconnected

information systems. Thus, efforts may focus on establishing a risk assessment and management process also through the implementation of public-private partnerships with ICT companies.

Starting the lower level possible, training of both civil servants and citizens need to be enforced, since knowledge and behavior of end-users are the first lines of defence against cyber-threats.

Analyzing several core documents and the steps that both EU and Japan are making towards developing eGovernment and especially implementing public electronic services, it can be noticed that improvements could be performed in regulating and better protecting this sector that involve dealing with sensitive data. On this respect, dedicated measures shall be designated and implemented. Dealing with highly sensitive data may need some procedure to include this domain on the list of critical infrastructures and to accordingly plan a strategy of cyber defence.

Japan's Strategy seems to be more articulated on the domain investigated by this research paper. While EU is proposing mainly a general framework, Japan is making the steps toward more specific cyber defence policies related to our topic of interest.

Although EU and Japan are working on the enhancement of eGovernment and electronic public services, their approach is slightly different. EU strategy was more focused on going in the same time with proposing, piloting and implementing several public services (cross-border), without ensuring first the adoption of the core e-service, the eID. Japan decided to go first for what EU calls "eID" and then based on it to implement several electronic public services. What seems to lack to both approaches are dedicated and more targeted measures to face the challenge of cyber threats. Experiences from both systems could serve as a basis for improvement of eGovernment and for the proposing of dedicated global cybersecurity principles and actions.

Acknowledgement: I would like to express my acknowledgement for supporting this research to Professor Motohiro Tsuchiya (Keio University), Professor Hirokazu Okumura (University of Tokyo), Mr. Kenji Hiramoto (Cabinet Secretariat), Mr. Toshiyuki Zamma (Cabinet Secretariat, MIC), Dr. Ikuo Misumi (NISC) and Mrs. Yuka Sasagawa (University of Tokyo).

References:

1) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN (2013) 1 final - 7/2/2013
2) Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union – COM (2013) 48 final - 7/2/2013 - EN
3) Executive Summary of the Impact Assessment – SWD (2013) 31 final - 7/2/2013

4) Impact Assessment – SWD (2013) 32 final - 7/2/2013
5) http://japan.kantei.go.jp/policy/it/2015/20150630_full.pdf
6) http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf
7) http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf
8) European Programme for Critical Infrastructure Protection
9) Directive on European Critical Infrastructures
10) Jeong, C. H., 2007: Fundamental of Development Administration. Selangor: Scholar Press.
11) Millard J., 2011: The Global Rise of e-Government and Its Security Implications in Kim J. Andreasson (ed.), 2011: Cybersecurity: Public Sector Threats and Responses, CRC Press
12) Muhamad Rais and Nazariah, 2003: E-government in Malaysia. Kuala Lumpur: Pelanduk Publications, 70-71