Protect Critical Information Infrastructure Systems in Financial and Healthcare Sectors: Actor Network Theory

Cheng-Chieh Huang
Dept. of Information Management
National Taiwan University
Taipei, Taiwan
d94725007@ntu.edu.tw

Ching-Cha Hsieh
Dept. of Information Management
National Taiwan University
Taipei, Taiwan
cchsieh@im.ntu.edu.tw

***Abstract*—CIIP is not only instrumental means but also social relevance. Most of studies on CIIP neglect considering social groups that CIs or CIIs serve and social characteristics of technology. In this article, it proposes actor network theory to analyze interdependence of CIIs and CIIP policy. Finally, it indicates social dimension in interdependence analysis, government's broker role and social-technical service system approach in critical information infrastructure protection studies.**

Keywords-critical information infrastructure protection; actor network theory; service systems

I. INTRODUCTION

Critical infrastructure protection (CIP) is currently seen as an essential part of national security in numerous countries around the world and a broad range of political and ad-ministrative initiatives and efforts is underway in the US, in Europe, and in other parts of the world in an attempt to better secure critical infrastructures (CIs).

The CI delivers a range of services that individuals, and society as a whole, depend on. That is, any damage to or interruption of the CI could cause ripples across the technical and the societal systems. Moreover, the critical information infrastructure (CII) underpins many elements of the critical infrastructure, as many information and communication technologies (ICT) have become all-embracing, connect other infrastructure systems, and make them more interrelated and interdependent[1]. Critical information infrastructure protection (CIIP) forms new issues for policy research and technology studies.

Past literature on CIP or CIIP divided into two angles, one from technology or system angle to discuss interdependence of technology, infrastructure or cyber security protection [2][3]. Another discusses about public-private-partners or government role from policy research [4] [5].

These studies neglect that current digital economic society is an interwoven socio-technical seamless web, consisting of heterogeneous, changing formations of actor networks, meanings, work practices and institutional and organizational arrangements [6]. They forget social groups that these critical infrastructures or technology serve and technology finally become a part of the relevant practical, symbolic and cognitive spaces of the actors involved [9]. Thus, it seems to consider social, technology or infrastructure simultaneously in CIIP.

In this paper, we propose a social-technical perspective, Actor Network Theory (ANT) to understand the complex social, technology interwoven phenomenon of critical information infrastructures and their protection. Using ANT, we can get a deeper understanding of the interrelationships of heterogeneous actor groups and of the mediating roles played by humans and technologies, and the critical information infrastructures. Further implications to interdependence of critical information infrastructure, government involvement, and public-private-partnerships issues are also discussed.

In the following section, we first review the literature of CIIP. Second, we review ANT Theory. Third, the financial and healthcare sectors of our cases are illustrated. Fourth, we present analysis and discussion and fifth, we identify contributions, limitations and suggestions for future research.

II. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

CIs are part of a larger set of services and products that are considered essential to the functioning of our modern economies and societies. These include but are not limited to energy, information technology, telecommunications, healthcare, transportation, water, government and law enforcement, and banking and finance.

Critical Infrastructure Assurance Office (CIAO), an interagency office created under Presidential Decision Directive 63 to assist in coordinating the federal government's initiatives on critical infrastructure protection in US [3]. The CIAO defined infrastructure as:

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.

Most of the CI relies on a spectrum of software-based control systems for smooth, reliable, and continuous operation. In many cases, information and communication

 ISBN:978-1-61208-114-4

technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them interrelated and interdependent. These ICTs underpin many elements of the critical infrastructure, called Critical Information Infrastructures (CIIs)[1].

Complex and interdependence of CIs or CIIs are difficult to manage, even protect. Most of CIP or CIIP studies discuss systems of system or interlinks to protect. They define physical interdependency, cyber interdependency, geographic independency, logical independency to analyze or protect [2][3].

These studies provide good analysis tools or methods to protect technology or infrastructure systems. But they forget the final objective of CIP or CIIP to protect people or society that CIs or CIIs serve not just technology or infrastructure themselves. And these services that technology or infrastructure provide are different meanings for different users in their different sectors or stages of usage.

Moreover, there are different institutionally fragmented environments in different sectors of different countries such as healthcare, transportation, water and they serve different user groups and interests groups[1][4]. If we cannot understand meanings of users or interests groups of critical infrastructure in different sectors it serves, it is difficult for government representatives to persuade CEOs or CIOs of critical infrastructure companies to invest.

That is, it is more meaningful to consider society, technology and their interwoven simultaneously in the CIP or CIIP studies.

III. ACTOR NETWORK THEORY

The social-technical approach encapsulates a wide range of perspectives and concepts. They attempt to explain the relationship and interactions between technology and society.

Actor Network Theory (ANT) is one of the most important social-technical perspectives in recently years. It was developed in the sociology of science and technology school [10]. ANT helps describe how actors form alliances and involve other actors and use non-human actors (technology) to strengthen such alliances and to secure their interests. ANT consists of two concepts: translation and inscription.

When an actor-network is created, consists of four processes of translation [11]:

- Problematization: The focal actors define interests that others may share, establishes itself as indispensable resources in the solution of the problems they have defined. They define the problems and solutions and also establish roles and identities for other actors in the network. As a consequence, focal actors establish an "obligatory passage point" for problem solution which all the actors in an actor-network must pass.
- Interessement: The focal actors convince other actors that the interests defined by the focal actors are in fact well in line with their own interests. Through interessement the developing network creates sufficient incitement to both lock actors into networks.
- Enrollment: Enrollment involves a definition of roles of each of the actors in the newly created actor-network. It also involves a set of strategies through which focal actors seek to convince other actors to embrace the underlying ideas of the growing actor-network and to be an active part of the whole project.
- Mobilization: The focal actors use a set of methods to ensure that the other actors act according to their agreement and would not betray. With allies mobilized, an actor network achieves stability.

In addition to the four stages of translation, the process of inscription is critical to building networks, as most artifacts within a social system embody inscriptions of some interests. As ideas are inscribed in technology and as these technologies diffuse in contexts where they are assigned relevance, they help achieve socio-technical stability.

IV. CASE STUDY

A. Case Background

This case is a three years research project to understand the current critical information protection status of every sector in Taiwan. In every year, the research project team will generate CIIP strategies and policy implications reports for government.

In 2009, the first year of research project, the project team decided financial, healthcare sectors as first priority to examine. The project team adopted "sector roundtables methodology" [7] and table-top exercise to understand protection status and dependence or interdependence between sectors.

In every sector analysis, the project team introduced four steps: 1. select CIIs, 2. analyze threats, weakness and interdependence, 3. design exercises, 4. execute table-top exercises and get evaluations from experts.

Followings are the project experiences and reflection in financial and healthcare sectors in first year.

B. Financial Sector

In the financial sector, there are more than forty large banks and institutions in Taiwan. Most banks and institutions are privacy, but they are supervised by Financial Supervisory Commission of Taiwan government (FSCEY). Moreover, the most critical institutions, such as stock exchange institution, futures exchange institution, depository or cleaning institution are government funded.

There two subsystems or mechanism that serve different users. One is the stock exchange system that supports the investors to exchange stocks or futures in the stocks or futures markets. The institutions and information systems must make sure the fair trade and the price is sensitivity to any crisis or news. The actors or technology system should response quickly to any crisis.

 ISBN:978-1-61208-114-4

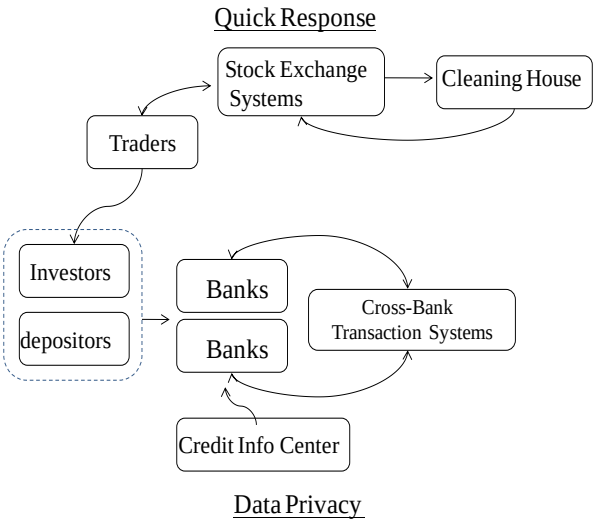

Figure 1. Subsystems in Financial Sectors

TABLE I. COMPARISONS OF ENERGENCE AND PRIVACY ISSUES IN FINANCIAL SECTORS

Institutions	Emergence Issues	Privacy Issues
Banks	Low	High
Clearning Hourse	Medium	Medium
Stock Exchange Institutions	High	Low
Credit Info Center	Low	High

Another subsystem is the banking system. The banks provide their customers to deposit or loan. Thus, compared to stock exchange system, data privacy is more critical for the banking system than quick response. Even the cross-bank transaction system is shutdown; the customers still can withdraw money by branch of banks.

Thus, the two subsystems represent their different protection angles. The stock exchange system focus on when and what sequences they should stop the exchange markets and announce to people or inventors. The banking system protects their data and prevents data leak from their inner control mechanisms.

No matter banks, stock exchange instructions, they very depend on information systems. They are also very actively response to any events that will impact confidence of people or their investors.

For financial sector, inscriptions of their CIIs are "confidence" and their cultures are responsively to serve their customers.

Thus, they expect the electrical power or telecommunication could recover quickly and response the exactly recover time to satisfy their customers' expectation.

C. Healthcare Sector

TABLE II. COMPARISONS OF ENERGENCE AND PRIVACY ISSUES IN HEALTHCARE SECTORS

Institutions	Emergence Issues	Privacy Issues
Hospitals/Clincals	Low	High
Heathcare insurance institution	Low	Medium

Although in the healthcare sector, such as hospitals or clinics are also the service institutions to serve their customers. But they are less IT resources to operate because of most resources are invested in clinical instruments. A Chief Information Officer (CIO) of a hospital said, "Our IT problem is less IT resources. We do not have enough IT investments and also we do not have qualified IT people to join".

"One day, our data center flooded because of a typhoon. We wait for one week to get the electrical power engines to recover our electronic power and data center!" the CIO updated. Also, if some accidents that let MIS people cannot work, such as H1N1 infection could be a problem to run IT operation.

The hospital information systems (HIS) are critical information systems, but it will bring just inconvenient, such as register or submit prescription slowly while IT breaking down. Also, clinical information is very important; it is the data protection issue.

Other important institutions in health sector are health insurance institutions. There is only one health insurance institution in Taiwan and governed by government. While the healthcare insurance system is shutdown, the patients still can see a doctor, the hospitals or clinics can record their insurance numbers and issue later when the system is recovered. The health insurance institution holds partial clinical information in their database; it has some data privacy protection issue.

For healthcare sector, inscriptions of their CIIs are "convenient". And they spend little money on IT investments.

V. ANALYSIS AND DISCUSSIONS

It summarizes different inscriptions, problems, interests and requirements for dependent sectors in financial and healthcare sectors in table III. We can understand that different institutions concern their interests in every sector. Moreover, the technical elements, CIIs also represent their different meanings, such as 'confidence' or 'convenient. Before protection policy carried out, we should understand relevant social groups in sectors, their meanings and social inscriptions of technology.

Following sections, we discuss new insights and implications of CIIP from the ANT theory.

 ISBN:978-1-61208-114-4

TABLE III. ANT ANALYSIS IN FINANCIAL AND HEALTHCARE SECTORS

ANT Analysis/ Sectors	Financial-Stock Exchange Subsystem	Financial-Banking Subsystem	Healthcare
Inscription	confidence	confidence	convenient
Translation (problems and interests)	reover market confidence quickly	data protection and confidence	smooth healthcare process, less IT resources

A. *Social Relevance, then Protection*

Most CIP or CIIP literature focuses on analyzing different interdependences of CIIs in different sectors. But they neglect how they collaborate under their different interdependence or dependences relationships.

For example, in our project experiences, the stock exchange subsystem in financial sector very depend on electrical power, and request that every shortage power events, the electrical power company should response planned recovery time quickly.

For institutions in financial stock exchange subsystem, transparent and confidence information they provide to their investors are important in financial markets. But for the electrical power company, they concern not only recovery quickly, but electrical power stable and quality.

Usually, the CIIs are dependent or interdependent, but their social concerns are inconsistent.

Thus, how to enroll the "confidence" CIIs of financial sectors and "stable" CIIs of electrical power sectors is not only from system functional views but from the social-technical angle.

B. *Redefine Government's Role in CIIP*

It is difficult for policy makers to enroll the private sectors to join the critical information infrastructure protection actor-network. Especially, private sectors realize the governments want they invest in security and reliability beyond their normal business continuity requirements [4]. Moreover, what is the government's role in CIP or CIIP?

From ANT analysis, the different sectors have their different competition environments, relevant social groups, social-technical configurations, and meanings. It is not suitable for policy makers to persuade or enroll these actors from only "national security" reasons or strategies.

ANT theory argues that focal actors establish an "obligatory passage point" for problem solution which all the actors in an actor-network must pass. It means governments as the focal actors, should consider obligatory passage points for sectors or institutions to enroll.

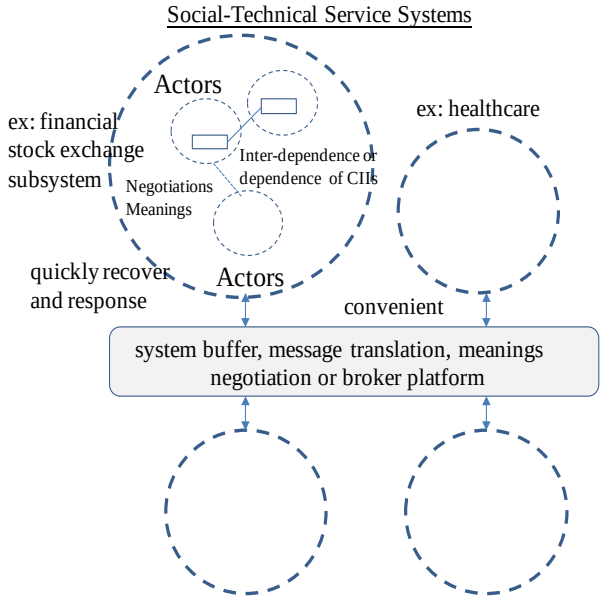

Figure 2. The Social-Technical Service System Apporach to CIIP

For example, "confidence" is the financial sector's consideration to their IT investment. The policy makers should persuade or assist they to strength these mechanisms or technologies. Few resources are the problems to healthcare sectors, how to allocate different resources while crisis happened is solution to enroll healthcare sectors.

Moreover, as our cases showed, these sectors depend on other sectors' technologies or infrastructures, but pursue themselves interests. Government could provide the broker role or build up boundary infrastructures, to help different sectors to collaborate or negotiate.

Thus, we call this kinds of relationships should be private-public-private partnerships.

C. *Methodology of CIIP*

Developing a comprehensive architecture or framework for interdependency modeling and simulation is very challenge. Moreover, it is difficult to resolve different sectors' problems using a single methodology or analysis tool.

No matter what kinds of tools or methods, it should consider more on social-political dimensions. Moreover, these methods should not try to sacrifice sectors' or actors' interests, but how to strength or broker their interests or meanings.

In summary, we propose the "Social-Technical Services Systems" view to guide the methods design (see figure 2). It provides the service system view to understand every sector or subsector service meanings, requirements. Also, governments or institutions can provide the broker roles or information system platforms to help negotiate different meanings, translate requirements to help every sectors achieve their obligatory passage points.

 ISBN:978-1-61208-114-4

VI. CONCLUSION

In this article, we propose the actor network theory to understand complex social, technology interwoven phenomenon of critical information infrastructures and their protection. Through our financial and healthcare sectors experiences and social-technical analysis, it implicates that include social dimension in independence analysis. Moreover, governments should also consider sectors' interests, and play a broker role to balance or negotiate their different interests. Finally, we propose social-technical service system approach to protect critical information infrastructure.

Future research, we will take more in-depth analysis of different sectors about their meaning, negotiations, interactions, interests, and inscriptions. Finally, we will design more comprehensive methods for CIIP from a social-technical service system approach.

REFERENCES

[1] Brunner, E.M. and M. Suter, International CIIP Handbook 2008 / 2009, ETH, 2008.

[2] E. Bagheri and A.A. Ghorbani, "The State of the Art in Critical Infrastructure Protection: a Framework for Convergence", International Journal of Critical Infrastructure, 2007, pp. 1-36.

[3] S. M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, "Complex Networks: Indentifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, 2001, pp. 11-25.

[4] M.B. Bruijne and M. Eeten, "Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment", Journal of Contingencies and Crisis Management, 2007, pp. 18-29.

[5] M. Dunn, "The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)", International Journal of Critical Infrastructure, 2005, pp. 258-268.

[6] R. Kling and R. Lamb, "IT and Organizational Change in Digital Economies: A Socio-Technical Approach", Computer and Society, 1999, pp. 17-24.

[7] Dunn, M. and V. Mauer, International CIIP Handbook 2006, ETH, 2006.

[8] T. F. Pinch and W. E. Bijker, "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and Technology Might Benefit Each Other", Social Studies of Science, 1984, pp. 399-411.

[9] K. H. Sorensen and R. Williams, Shaping Technology, Guiding Policy, MA: Edward Elgar Publishing, 2002.

[10] M. Callon and B. Latour, "Unscrewing the big Leviathan", in Advances in Social Theory and Methodology, K. Knorr-Cetina, and A.V. Cicourel, Eds, London: Routledge & Kegan, 1981, pp. 277–303.

[11] M. Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay", in Power, Action and Belief, J. Law, Eds, London: Routledge & Kegan, 1986, pp. 197–233.

 ISBN:978-1-61208-114-4