Infrastructure Protection in the Dutch Financial Sector

Matthijs Van Oers, Leon Strous, Ron Berndsen

Chapter 9

INFRASTRUCTURE PROTECTION IN THE DUTCH FINANCIAL SECTOR

Matthijs van Oers, Leon Strous and Ron Berndsen

Abstract This paper presents a case study of critical infrastructure protection in the Dutch financial sector. The organizational structures are examined to discern the roles and functions that facilitate public-private cooperation. An assessment of the organizational structures is provided along with a description of how key organizations are identified. Finally, a basic model is presented that can be used by other sectors as a template for determining the appropriate organizational structures for critical infrastructure protection.

Keywords: Financial sector, protection, payments and securities systems

1. Introduction

After the September 11, 2001 terrorist attacks in the United States, the Dutch Government sent a letter [7] to the Dutch Parliament that included an action plan for anti-terrorism and safety [6]. This plan formed the basis for critical infrastructure protection efforts in The Netherlands and resulted in a detailed 2005 report [8] that described the critical sectors, their vulnerabilities, existing protective measures, new measures and follow-up actions. This report was used as the foundation for sector-specific efforts on critical infrastructure protection, including efforts in the financial sector.

Although critical infrastructure protection efforts initially focused on anti-terrorism and safety, the goal of critical infrastructure protection has evolved to include resilience in the face of disasters and other events as well as mitigating their risk and impact. For example, the threat of flooding, which is highly relevant in The Netherlands, is considered to lie within the scope of critical infrastructure protection.

Critical infrastructure protection is an essential activity for public and private entities. Issues that need to be addressed in a successful critical infrastructure protection approach are: (i) scope of protection; (ii) appropriate or-

Figure 1. Financial sector protection concepts.

ganizational structures; (iii) required levels of protection; and (iv) measures required to achieve the required levels of protection. Solutions that address these issues are by no means straightforward and different solutions exist for different sectors and different countries.

This paper presents a case study of critical infrastructure protection in the Dutch financial sector. The organizational structures for critical infrastructure protection in The Netherlands are provided along with an assessment of their effectiveness. A general model for critical infrastructure protection that is applicable to other sectors is also presented. Note that the emphasis is on sector-specific issues, not on the more general functions of government (e.g., disaster and crisis management by police forces and other emergency services).

2. Dutch Financial Sector Approach

This section provides an overview of the critical infrastructure protection approach adopted by the Dutch financial sector.

2.1 Sector-Specific Protection

The first phase of critical infrastructure protection efforts in The Netherlands occurred from 2001 to 2005. The government and stakeholders, including The Netherlands Bank (DNB) (also known as the Dutch Central Bank) produced a report [8] that defined and identified: (i) the critical infrastructure as a whole; (ii) critical sectors; (iii) critical products and services in the critical sectors; and (iv) critical points.

Included in the report were major risks and vulnerabilities with regard to the financial sector (e.g., terrorism, natural hazards and cyber crime). Note that financial risk is not within the scope of critical infrastructure protection – the financial risk of individual institutions is specifically addressed by prudential supervisors whereas overall financial stability is primarily the responsibility of the central bank. The Netherlands Bank introduced the concept of the financial core infrastructure (FCI), which comprises the most important institutions in the Dutch financial sector. Figure 1 highlights the main concepts related to financial sector protection in The Netherlands from the broadest to the most specific.

The Dutch critical infrastructure encompasses the sectors that, if disrupted, could have a serious impact in terms of human casualties, economic losses and/or societal upheaval. Within the financial sector, payments and securities are identified as critical products and services. The critical points are defined

as the buildings, installations, systems and geographical regions that are necessary for delivering the critical products and services. Note that critical points, which include large data centers that provide services to financial institutions, are not necessarily owned by FCI institutions nor are they under financial regulation. For security reasons, the list of critical points is not publicized by the government.

2.2 Critical Products and Services

A financial infrastructure protection working group established in 2005 identified payments and securities as critical products and services in the Dutch financial sector. Although a disruption of the payments and securities infrastructure would not directly lead to human casualties, a major outage could have serious consequences, including societal upheaval.

The payments and securities domain can be categorized as: (i) retail payments; (ii) wholesale payments; and (iii) securities. The distinction is intended to emphasize the differences with respect to products, customers, institutions and regulators.

- **Retail Payments Domain:** This domain consists of payment systems, products and services for consumers and corporations, along with the accompanying infrastructures. Examples of products are debit cards, credit cards, money transfers, cash payments and direct debits. Institutions involved in processing retail products are banks, automated clearing houses (ACHs) and payment settlement infrastructures.

- **Wholesale Payments Domain:** This domain consists of the inter-bank payment infrastructures and actors involved in large value (low volume) payments, foreign exchange and other money market products. Institutions involved in processing wholesale payments include operators of settlement systems, banks and institutions that conduct foreign exchange transactions (e.g., CLS).

- **Securities Domain:** This domain consists of trading platforms for equities and derivatives and the accompanying clearing and settlement infrastructures along with their various actors. The institutions include exchanges (e.g., NYSE Euronext) and clearing and settlement infrastructures (e.g., LCH Clearnet, EMCF and Euroclear).

Note that the payments and securities infrastructure is international in its scope and is very reliant on information and communications technology. Indeed, many financial organizations deliver cross-border services to a multitude of customers. Interested readers are referred to [4] for a detailed description of the various products and services at the European level.

2.3 Dutch Financial Infrastructure

The 2005 financial infrastructure protection working group established an initial list of critical institutions. However, the working group did not develop a formal method to evaluate institutions on a recurring basis. In the following, we describe the method for listing an institution as an FCI.

The Netherlands Bank is responsible for compiling the FCI list in collaboration with the Ministry of Finance and the Netherlands Authority for Financial Markets. The following qualitative criteria are used in the determination:

- Disruption of the institution leads to large economic losses or large-scale civil unrest.
- The institution is directly supervised and regulated by the appropriate Dutch authorities, namely The Netherlands Bank and the Netherlands Authority for Financial Markets.

Institutions are added to the FCI list if their total transaction volume or value is in the top 80% of all financial institutions. The application of the criteria identified six institutions in the retail payments domain, five in the wholesale payments domain and seven in the securities domain, yielding a total of fourteen institutions in the Dutch FCI list (some institutions are listed in more than one domain). Note, however, that The Netherlands Bank has the discretionary power to add or remove an institution if special circumstances warrant.

An organization identified as an FCI is susceptible to the following additional regulatory requirements:

- Compliance with The Netherlands Bank Business Continuity Assessment Framework [9].
- Participation in the financial sector's Crisis Management Organization to address operational disruptions of the payments and securities infrastructure.
- Participation in the Dutch terrorism alert system.
- Participation in meetings of the Business Continuity Platform for Critical Infrastructure Protection.
- Participation in market-wide simulation exercises.

Critical points can be, but are not necessarily part of, institutions in the FCI list. The identification of critical points is primarily the responsibility of FCI institutions as part of their regular risk managements and business continuity processes. Note that specific arrangements are made for critical points that are deemed essential to the entire financial sector (e.g., Swift, which provides secure financial messaging services).

2.4 International Context

The starting point for critical infrastructure protection is often a nationally-driven program. However, many financial market infrastructures operate across international borders. Indeed, regulation and oversight are often considered per institution and not per country. In the financial sector, oversight is a central bank function whose goal is to mitigate systemic risk while contributing to the smooth operation of the payments system. For example, crisis management of Target2, the European real-time gross settlement system for inter-bank payments, is led by the European Central Bank in collaboration with the other Eurosystem central banks.

In the European context, critical infrastructure protection in the financial sector focuses on the most important institutions in the European Union. This set includes all the institutions that have been identified by their home countries as critical.

2.5 Organizational Structures and Measures

After defining the scope of protection, the next step is to determine the organizational structures, adequate level(s) of protection and appropriate protection measures. In most cases, organizations leverage structures that are already in place and modify them as required to incorporate critical infrastructure protection tasks. Developing the right organizational structures for critical infrastructure protection within a sector, however, does present some challenges. Commercial parties are driven by profit and are not always prepared to invest in projects that add costs. Additionally, organizations are reluctant to share information necessary for critical infrastructure protection efforts to external entities, especially competitors. Overcoming these challenges demands a government authority or regulator to take a lead role. Also, the organizational structures should strike a balance between the demand for resources and the ability to obtain tangible results.

The development of measures for protecting critical infrastructures typically draws on experience, relevant events and historical data. This approach, however, is not well suited to dealing with events that manifest themselves only a few times in history such as a pandemic or the September 11, 2001 terrorist attacks. Indeed, the Fukushima nuclear disaster in 2011 demonstrates that historical information does not provide adequate guidance for protecting against unexpected events.

The success of a critical infrastructure protection approach is strongly influenced by the organizational structures and protective measures. The organizational structures can be categorized as: (i) public; (ii) public-private; and (iii) private. The protective measures can be divided into two types: (i) preventative measures that increase the resilience of critical processes; and (ii) corrective or responsive measures that decrease the impact of a crisis.

The Dutch financial sector engages a mixture of organizational structures and measures to enhance FCI resilience (Table 1). Note that this paper focuses

Table 1. Summary of national organizational structures and measures.

Structure	Category	Measures
Public	**Preventative** Prudential Supervision; Oversight; The Netherlands Bank	**Preventative** Business Continuity Assessment Framework; Supervisory Standards
	Ministry of Finance; Intelligence Agencies	Policy Reports; Threat and Vulnerability Analysis
Public-Private	**Preventative** Business Continuity Platform	**Preventative** Information Sharing Best Practices Consultation on Standards
	Terrorism Alert Working Group	Anti-Terrorism Measures; Terrorism Alert System
	Cross-Sector Collaboration	Cross-Sector Exercises
	FI-ISAC	Cyber Crime Data Exchange
	Sector Crisis Management	Market-Wide Simulation Exercises
	Corrective/Responsive Sector Crisis Management	**Corrective/Responsive** Crisis Management Decision- Making and Communication; Disaster Recovery Planning
Private	None	None

on the financial sector; therefore, other actors (e.g., Ministry of Interior and Ministry of Justice and Security) are not included because their relevance to the organization and implementation of critical infrastructure protection is not sector-specific. The same is true for protection measures such as the organization of special anti-terrorism police forces and the strategic stockpiling of oil and diesel in case of shortages.

Public Structures. The financial sector is subject to many regulators and policy makers. The most relevant global entities are the Bank for International Settlements (BIS), Financial Stability Board (FSB) and International Organization of Securities Commissions (IOSCO). At the European level, the entities include the European System of Central Banks (ESCB), European Banking Authority (EBA) and European Securities Markets Authority (ESMA). The Dutch entities include The Netherlands Bank (DNB), Ministry of Finance and Netherlands Authority for Financial Markets (AFM).

Although regulators and policy makers have different scopes, objectives and approaches, all of them have the common goal of financial sector stability. The institutions and organizational structures issue standards (e.g., guidelines, rec-

ommendations, principles and expectations) and/or perform supervision and oversight. The supervisors and overseers regularly assess the operational reliability, security and business continuity against the standards.

FCI institutions must comply with the requirements of The Netherlands Bank Business Continuity Management Assessment Framework [9]. These principle-based requirements address several areas: strategy and policy, business impact analysis and risk analysis, scenarios and measures, testing and monitoring, management and maintenance, and crisis management and communications. The principal-based requirements leave options for institutions to develop their own solutions, unlike rule-based requirements that prescribe exactly what must be implemented.

Additionally, the Ministry of Finance, The Netherlands Bank and Dutch intelligence community collaborate closely on critical infrastructure protection initiatives. These entities develop policy reports and perform threat analyses on a regular basis.

Public-Private Structures. There are two main reasons for establishing public-private partnerships for critical infrastructure protection. The first is that critical infrastructures incorporate both private and public investments; protecting these infrastructures is the task of the central government and requires collaboration with private sector asset owners and operators. The second reason is that public-private partnerships facilitate the management of cross-sector dependencies. The financial sector, for example, is heavily dependent on the telecommunications and energy sectors. Cooperation is required in order to optimize the level of protection. Cross-sector cooperation can also occur in private partnerships, but experience has shown that some form of public interaction or initiating force is key to success.

The following public-private partnerships have been instituted in the Dutch financial sector:

- **Business Continuity Platform for the Critical Infrastructure Financial Sector (BC-CIF):** The Netherlands Bank initiated and currently chairs this platform whose goal is to share knowledge and best practices on business continuity and crisis management between FCI institutions and with the Ministry of Finance. The platform serves as a coordination point for the financial sector with regard to governmental critical infrastructure protection initiatives. Examples of the shared information are best practices related to outsourcing of critical processes and vendor requirements.

- **Working Group on Alerting to Terrorism in the Financial Sector (WAFS):** This working group was created to facilitate the exchange of information on terrorism threats, anti-terrorism measures and the terrorism alert system. The Netherlands Bank chairs the working group, which includes FCI institutions, intelligence agencies and the Ministry of Finance. The working group has developed and implemented anti-

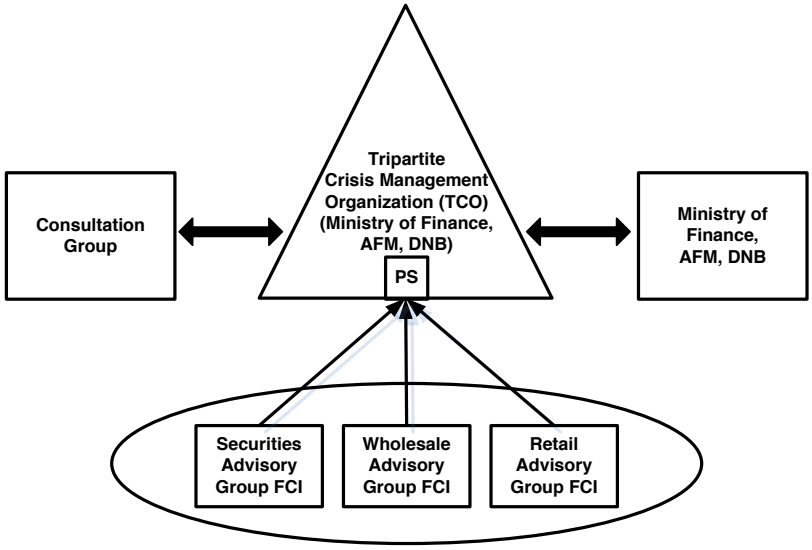

Figure 2. Crisis management structure.

terrorism measures that are activated depending on the threat level. The working group entities are connected to the terrorism alert system (organized, funded and operated by the government), which is designed to alert institutions in the critical infrastructure sectors to terrorist threats. Every critical sector in the Netherlands is connected to this system. Currently, the terrorism alert system is designed to warn of physical threats; however, efforts are underway to extend the system to include cyber threats.

- **Financial Institutions Information Sharing and Analysis Centre (FI-ISAC):** The goal of FI-ISAC is to exchange information between banks, infrastructures and government organizations in order to prevent and respond to cyber security incidents that could lead to fraud, loss of reputation and other risks. The FI-SAC works closely with the National Cyber Security Centre (NCSC).

- **Sector Crisis Management:** This sector-level structure is designed to perform corrective and responsive actions in the event of a major disruption to the payments and securities infrastructure. The structure comprises the Tripartite Crisis Management Organization (TCO), which incorporates the Ministry of Finance, Netherlands Authority for Financial Markets and The Netherlands Bank as board-level entities. A Consultation Group consisting of board members of FCI institutions, and various Advisory Groups provide recommendations to the TCO. The TCO is supported by a Permanent Secretariat (PS) that helps manage collaboration. Figure 2 presents the crisis management structure for the payments and securities infrastructure.

Table 2. Cross-border organizational structures and measures.

Structure	Category	Measures
Public	**Preventative** Oversight	**Preventative** CPSS-IOSCO Principles for Financial Market Infrastructures; Crisis Management Exercises
	Corrective/Responsive Eurosystem Crisis Management	**Corrective/Responsive** Crisis Management Decision-Making and Communication
Public-Private	None	None
Private	None	None

- **Cross-Sector Cooperation with the Telecommunications Sector:** In order to manage the effects of interdependencies in the financial sector, Platform BC-CIF started a collaboration with the National Continuity Forum for the Telecommunication Sector. An example of this collaboration is a jointly-organized crisis management exercise that seeks to strengthen cross-sector resilience.

Private Structures. No specific private partnerships related to critical infrastructure protection currently exist in the Dutch financial sector. However, a few structures have been created that indirectly support critical infrastructure protection goals. An example is a task force organized by the Dutch Bankers Association to address cyber crime threats.

2.6 Cross-Border Structures and Measures

Nationally-oriented critical infrastructure protection is limited because the majority of the financial market institutions operate across national borders. Indeed, critical infrastructure protection in the financial sector is quite complex with regard to coordination, legal aspects, ambiguities of roles and responsibilities, and vulnerabilities. Currently, the only cross-border collaborations that exist are public-only partnerships involving the European System of Central Banks and the Bank of International Settlements (BIS). These entities coordinate oversight, standard setting and crisis management activities across the Eurozone, European Union as well as globally. An example standard is the CPSS-IOSCO Principles for Financial Market Infrastructures [2].

Table 2 summarizes the cross-border collaborations and structures related to critical infrastructure protection in the financial sector. Clearly, cross-border coordination is still in its infancy and is an area that needs improvement.

2.7 Challenges

In general, critical infrastructure sectors are relatively easy to identify (e.g., energy, telecommunications, finance and health care). However, in some sectors, it is difficult to identify the critical services and processes, institutions and components. This is often the case in a highly networked infrastructure where small components can be essential to the overall function.

A large number of critical components in a sector can render it difficult to manage effectively. Alternatively, a small number of critical components can induce neglect and complacency with regard to overall critical infrastructure protection efforts. It is important to recognize these situations and strike the right balance when prioritizing assets.

In the case of a major disaster that impacts multiple sectors such as energy and telecommunications, services from the various sectors tend to recover at different rates. This may create serious problems when one sector is dependent on another. Due to resource limitations, sectors must set priorities according to the most critical societal functions and contractual obligations.

To increase the resilience of the critical infrastructure, it is recommended to maintain the transparency of priorities to the extent possible. Transparency facilitates preparatory efforts that lessen the impact of a disaster and helps clarify the lines of responsibility of public and private sector entities.

Finally, critical infrastructures are becoming more complex, more interconnected and, in many cases, they extend beyond national borders. These developments increase the difficulty in defining organizational structures for critical infrastructure protection. Indeed, there is an urgent need to address this issue going forward.

3. Analysis

Significant critical infrastructure protection efforts have been undertaken in the Dutch financial sector. The question is whether these efforts have resulted in effective organizational structures for critical infrastructure protection.

Assaf [1] has shown that intervention with regard to critical infrastructure protection efforts ranges from pure state provisions to pure market-driven provisions. The types of intervention are identified as: command and control, delegation to agency, delegation to agency plus negotiations, enforced self-regulation and voluntary self-regulation.

The choice of the level of intervention is based on the distinction between two regulatory models for critical infrastructure protection, the national security model and the business continuity model. The national security model focuses on security and public safety, and leads to critical infrastructure protection with a preference for government intervention. The business continuity perspective is based on neoliberal economic values. Business continuity is viewed in terms of return on investment and risk management; thus, the model results in a preference for market provisions. Although the two models may align in extreme cases, they have competing sets of values that result in differ-

ent regulatory interventions. Also, as mentioned above, the differences in goals and approaches between the private sector and the public sector can also be explained from an externality perspective.

A hybrid critical infrastructure protection approach is implemented in the Dutch financial sector. For some critical infrastructure protection functions, strong government intervention exists (e.g., supervision and oversight based on legal provisions). For other functions, voluntary self-regulation exists (e.g., determining business continuity best practices and vendor requirements). This hybrid approach also addresses accountability and transparency associated with critical infrastructure protection efforts. If a high degree of accountability is needed, strict government intervention must exist; self-regulation is appropriate if trust is the most important component of the public-private partnership.

The validity of the hybrid critical infrastructure protection approach adopted by the Dutch financial sector is further strengthened by Dunn-Cavelty and Suter [3]. They argue that public-private partnerships in which the public parties have a strong role are not always optimal. Indeed, information sharing is considered to be the most important requirement for critical infrastructure protection. Information sharing requires complementary goals, mutual trust, clear distribution of risks, clear sharing of responsibilities and authority, and market- and success-oriented thinking [5]. Because of concerns related to confidential information and the divergent goals of national security versus business continuity, a strong government role may hinder effective information sharing in some critical infrastructure protection functions. Indeed, an approach where the government takes on a "meta role" is sometimes required. In such a scenario, the government is not focused on monitoring the collaborating organizations, but instead coordinates and stimulates functional networks so that the organizations can fulfill the tasks required by the state.

In the Dutch financial sector, The Netherlands Bank assumes the coordination and stimulation roles for several tasks (e.g., Platform BC-CIF). Meanwhile, the financial sector uses FI-ISAC for sharing information related to cyber security. Thus, for aspects that require a national security model, a more government-interventionist organization has been chosen by the Dutch financial sector. On the other hand, for business continuity, where information sharing is key, a low-interventionist, public-private partnership model has been selected.

4. Proposed Model

Our model for determining organizational structures for critical infrastructure protection is derived from the Dutch financial sector efforts described above. The model, which is illustrated in Figure 3, incorporates three steps:

- **Define:** The initial step in a critical infrastructure protection program is to define the scope of protection, critical processes, products and services. Additionally, a global risk analysis must be performed to identify the major vulnerability concerns. This step is project-based and requires the collaboration of public and private sector entities.

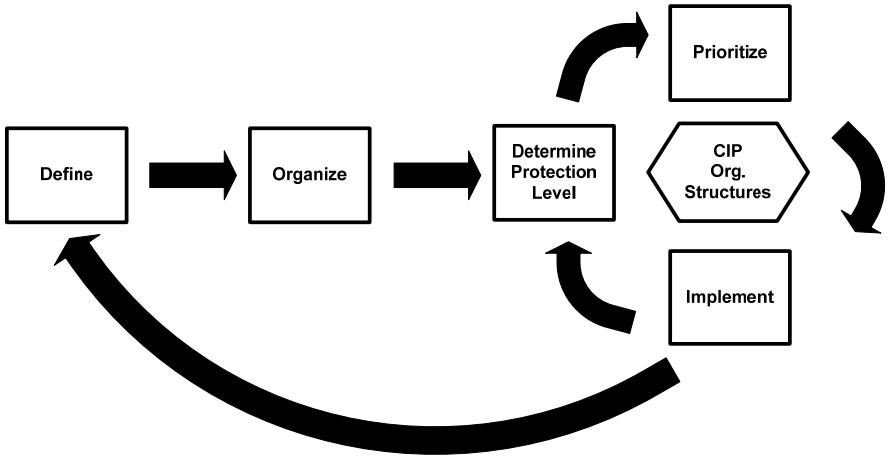

Figure 3. Model for determining organizational structures.

- **Organize:** After the definition step, it is necessary to set up the organizational structure. The organization of public-only and public-private partnerships in a sector should cover four themes: (i) anti-terrorism; (ii) business continuity based on an all-hazard approach; (iii) information and communications technology; and (iv) crisis management. These themes typically cannot be addressed by one organization because they require different decision-making mandates and/or expertise. It is, however, important to manage the intersection of the themes. The institutions that are in charge of these organizational structures should be aware of topics that cross multiple themes and a model of collaboration should be considered, ranging from pure government intervention to pure self-regulation. After these organizational structures are established, efforts to protect the infrastructure can proceed.

- **Determine Protection Level, Prioritize and Implement:** The next phase involves determining the protection levels and priorities and proceeding with the implementation. These tasks are executed by dedicated critical infrastructure protection structures (hexagon in Figure 3).

  During the determination of protection levels, preventative, corrective and response measures are also identified based on risk analysis. Following this, the priorities for implementing protection measures are determined. The setting of priorities is often influenced by statistical information about events, threats and risks, cost-benefit tradeoffs, political and societal influences, and the latest crisis. After the priorities are set, the FCI institutions implement the required protection measures.

  It is important to note that the latest crisis invariably exerts an influence on critical infrastructure protection efforts. After the attacks of Septem-

ber 11, 2001, anti-terrorism efforts were increased. When the Mexican Flu broke out, The Netherlands took strong efforts to protect its citizens from the pandemic threat. The current focus is protecting the critical infrastructure from cyber attacks. These efforts are important and our intention is not to imply that they have received too much attention. Rather, we highlight this issue because it is important not to become myopic and dismiss other potential risks.

The proposed model is intended to be applied as a cyclical feedback loop. Changes within a step can propagate to affect subsequent steps. Therefore, it is essential to perform periodic reviews and updates to account for changes in the infrastructure and threat landscape.

The participation of at least one institution (e.g., regulator, government agency or private entity) that takes the lead in organizing the initial phase of a public-private partnership is a requirement. The institution should focus first on initiating collaboration in the sector and addressing the major concerns. After the initial coordination, a tailored approach for determining the appropriate public-private partnership can be developed.

5. Conclusions

The Dutch financial sector provides a concrete example of a sector-wide approach for critical infrastructure protection. The measures implemented by individual institutions along with sector-wide efforts appear to be very effective for safeguarding critical assets. The appropriate use of public-private relationships has fostered communication and information exchange, as well as the protection of sensitive information where necessary. Government intervention has been selected for functions in which national security is the primary consideration. On the other hand, a market-oriented approach is employed for functions that rely on sharing and trust. The basic model derived from the Dutch financial sector can be used as a template by other sectors – or other countries – to determine the organizational structures that can achieve effective critical infrastructure protection.

Our future research will conduct further analysis of critical infrastructure protection in the Dutch financial sector and refine the model as appropriate. Also, it will attempt to model and analyze cross-sector and international collaborative activities related to critical infrastructure protection.

References

[1] D. Assaf, Models of critical information infrastructure protection, *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 6–14, 2008.

[2] Committee on Payment and Settlement Systems, Payment and Securities Principles for Financial Market Infrastructures, Bank for International Settlements, Basel, Switzerland (`www.bis.org/publ/cpss101a.pdf`), 2011.

[3] M. Dunn-Cavelty and M. Suter, Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, vol. 2(4), pp. 179–187, 2009.

[4] European Central Bank, The Payment System, Frankfurt, Germany (www.ecb.int/pub/pdf/other/paymentsystem201009en.pdf), 2010.

[5] V. Kouwenhoven, Public-private partnership: A model for the management of public-private cooperation, in *Modern Governance: New Government-Society Interactions*, J. Kooiman (Ed.), Sage, London, United Kingdom, pp. 119–130, 1993.

[6] Ministry of General Affairs, Actieplan Terrorismebestrijding en Veiligheid (in Dutch), The Hague, The Netherlands (zoek.officielebekendmakingen.nl/kst-27925-21.html), 2001.

[7] Ministry of General Affairs, Brief van de Minister-President, Minister van Algemene Zaken en van de Ministers van Justitie, van Binnen-Landse Zaken en Koninkrijksrelaties, Terroristische Aanslagen in de Verenigde Staten, Kamerstuk 27925, Nr. 10, Vergaderjaar 2001-2002 (in Dutch), The Hague, The Netherlands (zoek.officielebekendmakingen.nl/kst-27925-21.html), 2001.

[8] Ministry of the Interior and Kingdom Relations, Rapport Bescherming Vitale Infrastructuur (in Dutch), The Hague, The Netherlands (www.eerstekamer.nl/9370000/1/j9vviasdcklgjqj/vh4gfzjj2vqo/f=/vh4gfzjj2vqo.pdf), 2005.

[9] The Netherlands Bank, Assessment Framework for Financial Core Infrastructure, Business Continuity Management, Amsterdam, The Netherlands (www.dnb.nl/en/binaries/DNB\%20Assessment\%20Framework\%20Business\%20Continuity\%20version\%202011_tcm47-253700.PDF), 2011.