FSPOS

Finansiella Sektorns Privat-
Offentliga Samverkan

Crisis communication in the financial sector - guidelines in the event of major disruptions

Knowledge overview: Cyberattacks

FSPOS AG INFO

Table of contents

1. SUMMARY 3

2. INTRODUCTION TO THE GUIDELINES 4

3. COMMUNICATIONAL CHALLENGES 5

4. GUIDELINES ON CRISIS COMMUNICATION 7

5. KNOWLEDGE OVERVIEW: CYBERATTACK IN THE FINANCIAL SECTOR 10

APPENDIX A: A FOURSQUARE FOR A COMMUNICATIONAL OPERATING PICTURE 17

APPENDIX B: WORKING METHOD AND STRUCTURE - COLLABORATION MEETINGS 19

APPENDIX C – FSPOS MEMBERS AND ROLES IN A CRISIS 23

APPENDIX D: REFERENCE LITERATURE (IN SWEDISH) 27

1. Summary

The FSPOS Information Working Group, referred to here as *AG Information* (ArbetsGrupp Information), has drafted this report so that actors in the financial sector are well prepared to manage the communication undertakings that would be required if one or more FSPOS members were subject to a major cyberattack that might pose a threat to the financial system.

There are two reasons for drafting this report: Firstly, the financial sector and its infrastructure are based on complex IT systems that may affect financial stability in the event of a major cyberattack. Secondly, experience from the latest financial crisis in 2008 illustrates the importance of the sector having clear guidelines for its communication.

When the communication of banks and the authorities was evaluated in 2010, the sector was given credit for its communication during the acute phase of the crisis but received criticism of the way it communicated risks - in brief - too little, too late and not clear enough. Individual actors may also have exacerbated the crisis as a result of communicational mistakes[1].

AG Information[2] considers that the following principles should underpin communication in the event of a cyberattack or other major disruption that may pose a threat to the financial system and financial stability in Sweden:

- The actors concerned should be open, react quickly and be clear in their own crisis communication in the event of, for example, a cyberattack and ensure that this communication is well anchored in its own everyday operations.
- They should avoid situations where there is a lack of openness and communication as such situations risk fuelling rumours and increasing uncertainty, leading to a crisis being created.
- The actors concerned should collaborate to maintain communication that safeguards financial stability.

These guidelines provide more detailed advice in connection with the recommendation on crisis communication drafted in 2010. FSPOS has also published guidelines on crisis management. This report looks specifically at communication in the event of an attack.

[1] *http://www.fspos.se/siteassets/fspos/rapporter/2010/storbankernas-och-myndigheternas-kommunikation.pdf*

[2] *Apart from Handelsbanken, see the FSPOS website at fspos.se for a complete list of members.*

2. Introduction to the guidelines

In recent years, cyberattacks have increasingly been the cause of disruptions in society. A relevant example is the hacking of the Bangladesh Central Bank in 2016, in which over 80 million US dollars disappeared. Another example is from South Korea in 2013, in which three major banks were subjected to a cyberattack that caused about 30,000 computers and servers to crash.

The financial system is the economy's lifeblood and it is easy to imagine the rapid development of a full-scale crisis if it is no longer possible to pay bills or receive money or salary. This situation can also be exacerbated if banks and authorities are seen to be uncommunicative, as a lack of information leads to rumour and speculation. There is also the risk of an operative crisis developing into a financial one with all the internal challenges this would pose. This is why high demands for openness are placed on all the relevant actors in the financial sector.

To fulfil these demands, each actor, both private and public, should take their responsibility to communicate actively regarding their own operations. In the event of a serious cyberattack against the financial infrastructure, there should be an orderly structure to manage any conflicts of interest that may arise among actors. These guidelines are intended to facilitate the establishment of such a structure. Experience from the latest financial crisis and from recently performed exercises - in which cyberattack has been one of the elements - is an important starting-point. The guidelines are split up into three parts:

1. A section on **the communicational challenges** that should be dealt with in the event of a cyberattack or other major disruption. This is based on a joint discussion among banks, authorities and sector organisations. Here, we outline the specific traps for open and active communication that actors in the sector should avoid.

2. **Guidelines on the sector's crisis communication** in the event of cyberattack or other serious disruption that may pose a threat to the financial infrastructure or stability (templates can be found in the appendix).

3. A **knowledge review of cyberattack in the financial sector**, actors, approaches and consequences for the sector's joint communication. The section includes two case studies of relevant events in the United Kingdom and the United States.

3. Communicational challenges

A major cyberattack or other similar disruption can be expected to lead to complex conflicts of interest for the actors involved. This may be different short- and long-term interests, both for the actors themselves and for the sector as a whole. These challenges require us to have a joint approach and to agree on routines and methods for communication (see next chapter, *Guidelines on crisis communication in the event of cyberattack*).

3.1 Conclusions for coordinated communication

Crisis communication can be crucial to the successful management of all sorts of disruptions in society. In the event of a forest fire or flood, for example, communication helps to ensure the more efficient use of resources and enables the general public to help minimise the risks and consequences. The financial system is built more on trust, however. The stability of the system itself is built on confidence, which means that failed communication can actually be the root cause of the disruption itself. Successful communication, on the other hand, can be crucial to the solution.

- Efficiently coordinated communication in the event of a cyberattack or other shock to the financial infrastructure presupposes two things: Firstly, that every actor, private as well as public, takes responsibility to actively communicate regarding their own operations. Secondly, that there is common agreement among all the actors involved - supervisory authorities, financial institutions and suppliers – to be transparent regarding what is known, and most of all regarding what is not yet known.

- Actors need both their own internal routines between IT, communication and decision-makers, and to have good knowledge of the financial sector's joint routines for crisis communication. The goal should be to promote working methods that meet the challenges and ensure efficient crisis communication in the event of a major disruption. Collaboration on the need for a joint operating picture can be initiated by relevant actors but is led by the relevant authority (Finansinspektionen or the Riksbank depending on the nature of the disruption).

- Joint working methods need an orderly structure that allows for temporary expansion or contraction of the group, as it is hard to foresee exactly which counterparts will need to collaborate in case of an unexpected course of events. Cyberattack can lead to very complex situations with the need for communication across organisational, sector or national borders. In order to instil those involved with confidence, the coordination should be led by the relevant authority.

Reaching agreement and building trust are key to being able to safeguard financial stability in case of cyberattack. It is crucial that there is a common view on what is expected of each actor as well as a well-supported consensus on how information is to be shared. Agreements must also be anchored before the crisis becomes a reality – if a crisis has already broken out, it is too late.

3.2 *Traps to be prepared for and avoid*

Uncertainty about what can be communicated

When a cyberattack occurs, there is often considerable uncertainty to start with as to what has happened and how operations are affected. This uncertainty can have many root causes, for example it could be an external service provider who has been affected or several actors may be having problems.

There is hence a risk of actors delaying their external communication pending confirmation about what has happened and how serious the problems are. Such an approach can create an information vacuum that can be filled by other actors and lead to speculation and rumours that are hard to quash later on. If the cyberattackers have a prepared communication strategy as part of their influence operations, or to fulfil ideological goals, the risk of them succeeding increases.

Lack of openness as a result of internal processes and competition

An incapacity to communicate can have several causes. Whatever the reason, the consequence is that the organisation or sector is perceived as uncommunicative by customers, the media and the general public. One reason for this incapacity can be that cyberattacks are mainly seen as a technical problem. This can lead to difficulties not being reported to the board/management team quickly enough. Someone who fails to stem the problem may, in a worst-case scenario, be averse to notifying other parts of the organisation in order to avoid blame in the short term.

Another reason for a lack of openness can be a narrow-minded view on how much confidence people have in the sector. There may be short-term incentives to keep one’s distance when a competitor is exposed and loses money, or try to avoid to be the first to go public if one is affected oneself, which causes a tendency to shun cooperation and information sharing. The organisation thereby risks missing out on important information from other actors, fuelling rumours and speculation and increasing uncertainty.

Another reason for secrecy can be a lack of a holistic approach to the financial sector's dependencies and a lack of understanding of one’s own key role in society. Such conceptions can lead to a refusal to communicate, cooperate and share information with other actors. This can in turn lead to an event causing knock-on effects and negative consequences for the financial sector as a whole.

Overestimating a crisis

When a crisis is unavoidable, an actor can exaggerate how advanced the attack is, in order to give the appearance of it being impossible to defend against. This strategy can be seen as protecting oneself against criticism of having invested too little in information security and cybersecurity. Acting this way damages information exchange and makes it more difficult to establish a joint operating picture for the sector as a whole.

Underestimating a crisis

When a crisis is unavoidable, an actor can also *underestimate* how advanced the attack is and proclaim victory in advance. Authorities, media, customers and internal decision makers will push hard for the rapid reinstatement of the actor's functionality and for banking services, etc., to be back in stable operation. The temptation to communicate control over the situation in a complicated technical environment risks undermining the joint operating picture and can cause other parties to act based on an incorrect analysis. Long-term trust risks being damaged, in both the individual actor and the sector as a whole. In a similar way to the scenario described under the heading "Uncertainty" above, this can be particularly serious if the cyberattack is part of more extensive influence operations, where the attacker also has their own communication strategy.

Lack of a holistic perspective

A central challenge in the event of cyberattack is the risk that one actor's short-term interests may threaten financial stability, which also damages the individual actor in the longer term. A silo mentality between functions and actors creates a risk of decision makers, technicians and communicators performing worse collective analysis and assessments, which can lead to negative consequences for society at large.

4. Guidelines on crisis communication

4.1 The aim of the guidelines

These guidelines are based on the principles drafted in 2010[3]; openness, clarity, speed, accessibility and collaboration. More specifically, we stress here *how* the sector shall be able to communicate actively, transparently and clearly in a situation with great uncertainty and significant communicational challenges. The crisis we envisage is some form of major cyberattack that may threaten the financial infrastructure, although the guidelines are also useful in the event of other serious disruptions to the sector.

With good, coordinated crisis communication, actors in the financial sector can respond quickly to questions from the general public, customers and the media. This increases the chances of being able to counteract conflicting messages and rumours as well as of reducing the gap between the crisis and *the picture* of the crisis. Most important of all: Active and correct information alleviates the consequences of the disruption and thereby helps to maintain and strengthen both trust in the sector and stability in the financial system.

[3] *http://www.fspos.se/siteassets/fspos/rapporter/2011/rekommendationer_for_kommunikation.pdf*

The structured working method also makes sector actors better prepared for disruptions or crises that require coordination with actors in other sectors or when collaborating with other actors in the financial infrastructure.

The aim is for the guidelines to be used in the event of disruptions and crises that require strategic and coordinated crisis communication.

4.2 Basic assumptions

When collaborating on crisis communication in order to counteract attacks or major shocks in the financial sector, the following should apply:

- The actors concerned should be open, react quickly and be clear in their own crisis communication and ensure that this communication is well anchored in their own everyday operations.

- The relevant actors are responsible for signalling to the authorities, who can then initiate collaboration. There is common agreement among all actors to be transparent regarding what is known, and most of all regarding what is not yet known.

- We agree that it is perfectly possible to share and retrieve communicational operating pictures in order to obtain a better understanding of the event and at the same time respect the actors' respective roles in the financial system.

- We actively evaluate the effects of the communication.

4.3 Approach to active communication

- Communicating in a coordinated fashion does *not* mean saying the same thing but sharing one's operating picture with the responsible authorities and communicating transparently about the risks posed to one's own operations. It should be possible to share an operating picture even if it is obviously impossible to convey confidential information to a wider circle.

- All actors in the financial sector should behave and communicate in a way that helps strengthen robustness and maintain trust in the financial system in Sweden as a whole. To achieve this, all actors should strive towards being as open, clear, quick and proactive as possible in their external communication.

- Each actor is expected to be responsible for communication regarding their own operations and within their remit.

- Considerable emphasis is put on proactivity and collaboration between affected the relevant authorities and between authorities and private actors and sector organisations in order to safeguard trust in the financial system.

4.4 Preconditions for good crisis communication

The following makes it easier to achieve coordinated communication:

- Knowledge about each other's responsibilities, roles and information need before the unwanted event takes place.
- Consensus on what is worthy of protection within the sector from a societal perspective.
- A collective and communicative operating picture that will form the basis for decisions on communicational measures.
- Understanding of what information is required and how it is shared in a suitable way.
- Everyday communicator networks on both the strategic and operational level.
- Regular training and exercises that include crisis communication.
- Annually updated crisis plans and lists of contacts.

4.5 Working methods to coordinate communication

An agreed and practised working method enables actors together to quickly identify the situation, who should say what and how the sector together can build trust with the help of a proactive communication strategy. It is a question of creating a low threshold for collaboration and providing a structure for the work on drafting a joint communicational operating picture, see Appendix A.

All actors in the financial sector can initiate collaboration. Just one actor identifying a need for collaboration is sufficient to justify the collaboration. An individual bank does not need to host a collaboration conference itself, but has the responsibility for asking Finansinspektionen or the Riksbank to convene one.

5. Knowledge overview: Cyberattack in the financial sector

5.1 Experience and conclusions on communication

The exercise arranged by FSPOS in 2015 clarified a number of challenges that follow in the wake of a cyberattack and the importance of efficient crisis communication and collaboration[4].

Several actors felt that the collaboration at the time made it easier to manage the events in an efficient manner. All actors were open about their information and showed that there is a clear will to help each other within the sector.

Identified areas for improvement included how collaboration meetings were organised, conducted and followed up. It was unclear how the collaboration meetings should take place in practice, which led to less effective meetings in which joint operating pictures and coordinated messages could not be agreed on. There was little active coordination and reconciliation of messages, despite actors noting in the evaluation form that coordinating messages should make it easier to maintain trust among the general public in the event of a major incident.

One overall conclusion was that collaboration works best and is most effective when one actor has been assigned the responsibility to convene meetings, draft agendas, moderate, document and disseminate meeting minutes afterwards.

Surveys conducted by the Riksbank also show that many actors strive for increased collaboration in order to cope with cyberattacks. The majority of respondents call for increased collaboration and more information exchange in this area.[5]

This is also why members of AG Information agreed to perform an international knowledge review. In summary, it can be noted that collaboration has been highlighted as a central driver of effective communication in the event of international cyberattacks[6]. However, many financial actors said that they were not entirely comfortable with admitting vulnerability, loss and damage in an environment where the supervisory authority was present and where competitors could benefit from the information.

Even if efforts to strengthen collaboration in the financial sector are moving forward, the risk of well-resourced antagonists attacking several parts of the society poses major challenges. More complex attacks require the collaboration of a greater number of critical sectors in society.

[4] *http://www.fspos.se/siteassets/fspos/rapporter/2016/fspos-sektorsovning-2015---ovningsrapport.pdf*

[5] *http://www.riksbank.se/Documents/Rapporter/FSR/2016/FSR_1/rap_fsr1_160601_sve.pdf*

[6] *For a more detailed look at this, there are two case studies at the end of this section.*

5.2 *Description of cyberattack in the financial sector*[7]

The financial system is the economy's lifeblood and a central part of the infrastructure. It is also dependent on complex IT-systems, which makes it vulnerable to cyberattacks[8]. A shock in the financial system, caused by a cyberattack, can mean that the banks can no longer make payments to each other and perhaps not be able to pay out salaries on time. People might find it difficult to pay their bills, overall financial stability is affected and it may, in a worst-case scenario, lead to major economic costs (e.g. company bankruptcies and unemployment).

Cyberattacks against the financial system can also be combined with attacks against other sectors of society. An example of a wider disruption is the *"Dark Seoul"* cyberattack in South Korea in 2013. Three large South Korean banks were subject to a sabotage attack that caused 30,000 computers and servers to crash. This led to customers not being able to use online bank services and ATMs and some bank offices having to close. The systems of two large TV stations were sabotaged at the same time, which caused broadcast disruptions. This attack could be interpreted as an attempt at influence operations[9]. The fact that the act both disrupted banking services and made it more difficult for the general public to obtain information heightened the level of concern.

Attacks can be directed both against computers and mobile phones, regardless of the operating system. These can be overload attacks, aka DDoS (Distributed Denial of Service attacks) or DoS (Denial of Service attacks)[10], implementation of malicious code[11] or simple intrusion. Most threats are "bulk" attacks, which means that malicious code is distributed on a wide scale or that an attacker tries to identify vulnerabilities to facilitate wider attacks. Attackers may want to use the hacked system to distribute spam, for example. If a million e-mails containing malicious code are sent, they can create significant damage, even if only a fraction of the e-mails succeed in distributing the code.

In addition to these general attacks, that don't distinguish between targets, there are targeted attacks where the attacker designs the attack against a specific target. Targeted attacks are normally preceded by a phase where the attacker retrieves background

[7] *We wish to thank cybersecurity specialist Fredrik Hult, who has contributed to Sections 5.2-5.3 and the case studies.*

[8] *http://www.riksbank.se/Documents/Rapporter/FSR/2016/FSR_1/rap_fsr1_160601_sve.pdf*

[9] *For a definition of influence operations, see: Sid 41 https://www.msb.se/Upload/Nyheter_press/Rapport%20civilt%20försvar_2014_3277_slut.pdf*

[10] *The basic aim of a DoS or DDoS is to prevent normal access, although it can also be used to mask another ongoing attack. One type of attack is to overload the target with as much traffic as possible and consume all available bandwidth.*

[11] *Malicious code includes viruses (executable code that spreads among different systems), trojans (code that acts as a backdoor for further attacks), ransomware (code that encrypts files and forces the victim to pay money for access), spyware (code that retrieves information such as passwords or credit card information) and worms (code that replicates itself by utilising software security failures.*

information (e.g. names of key individuals), analyses internal processes, type of system and software versions in an attempt to produce the greatest possible effect.

5.3 *Actors behind cyberattacks*

Cyberattack can be a question of developing techniques to make traditional crime more effective or a "pure" cyberattack where the target and crime are digital. Such crimes include: theft of intellectual property rights, insider trading, credit card fraud, identity theft, bank payment fraud and blackmail.

Cyberattack is growing rapidly around the world and the United Kingdom estimates that it constituted 53% of all crime that was committed in the country in 2015, of which 36 percentage points is fraud-related cyberattack.[12]

Cyberattack focusing on payment infrastructure, blackmail viruses and sabotage has become more aggressive. An advanced cyberattack against the **Central Bank of Bangladesh** led to the theft of over 80 million US dollars. Similar attacks were directed also against other banks but with less success.[13]

Another example of international attacks against banks is those committed by the **Carbanak/Anunak-group** that is thought to have stolen more than a billion US dollars from over 100 banks. The group spent a long time, sometimes months, inside bank networks. They studied internal payment routines and identified which persons, functions and systems had control over the payment process. The attack was directed against banks payment infrastructure and personnel, not directly against its customer base. This has proved to be a very successful method as much of the security focus of the banks been on safeguarding internet bank transactions.[14]

Software vendors in the payments industry are another target for cyberattacks. A concrete example is the attack against **Micros**, one of the world's three largest vendors of payment terminals for credit and payment cards. As a result, cyber-criminals obtained access to payment systems in hundreds of companies.[15]

The larger criminal networks have moved their focus from attacks against customers' internet bank accounts towards blackmailing them through computer sabotage, a technique known as *"ransomware"*. Here the victim's documents and data are made unusable and inaccessible until a ransom has been paid out, often in the form of bitcoins in order to make tracking the money more difficult. The method is considered relatively

[12] *http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file*

[13] *http://www.bloomberg.com/news/articles/2016-03-18/hackers-stalked-bangladesh-bank-for-two-weeks-before-big-heist*

[14] *http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf*

[15] *http://www.ft.com/cms/s/0/657447a4-5d95-11e6-a72a-bd4bf1198c63.html#axzz4KkFrFDwn*

low-risk for the criminal. Internet bank attacks are more complicated and require the cyber-criminal to manage transactions, which makes them easier to detect.

Criminal marketplaces[16], where for example malicious code is sold, also allow ideologically driven actors to obtain the technology and put it to their own use. Political cyberattack is also part of the threat picture, where individuals and groups are driven by ideological reasons to sabotage, disclose business secrets or engage in some kind of digital vigilantism.

States can also carry out cyberattacks to influence opinion[17]. It is an increasingly well-established view that cyberattacks against civilian targets and publicly important functions are an integral part of modern warfare. Cyberattack can be used in order to destabilize a country's political system, spy on it or damage its economy. By attacking the financial sector, a state can cause another state substantial damage when part of the infrastructure is affected.

Some states are investing major national resources to develop advanced technologies, both to defend themselves against and to carry out cyberattacks. It can have major consequences for the financial sector if the technology falls in the wrong hands.

Case study 1: Cyberattack against US banks (Operation Ababil in 2012)

In September 2012, the internet and mobile bank services of several US banks crashed due to a DoS attack that has come to be known as "Operation Ababil"[18]. The attack continued for several weeks and to begin with, the banks found it difficult to protect themselves despite them being forewarned and threatened by a group of activists via the Pastebin website[19]. The group said that they intended to attack the US as a response to a controversial video uploaded to YouTube. Their stated goal was the New York Stock Exchange and a number of banks with operations in the US.

The Financial Services Information Sharing and Analysis Center (FS-ISAC), a voluntary body promoting collaboration between the public and private sectors, was responsible for coordinating and sharing information about the status of the crisis. They used a "traffic-light protocol" (TLP) for information sharing. This protocol makes it possible for members to choose different levels for how the information is spread by recipients.[20]

[16] *Examples of marketplaces include the now defunct Silk Road (http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/) and Evolution (https://krebsonsecurity.com/2015/03/dark-webs-evolution-market-vanishes/)*

[17] *Examples of this include the cyberattack against Estonia in 2007 (https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia) and the suspected Russian hacking of the Democrats email systems during the US presidential election campaign in 2016 (http://www.nytimes.com/2016/10/12/us/politics/obama-russia-hack-election.html?_r=0)*

[18] *https://security.radware.com/ddos-knowledge-center/ddospedia/operation-ababil/*

[19] *http://pastebin.com/mCHia4W5*

[20] *https://www.us-cert.gov/tlp*

The interbank cooperation within FS-ISAC was fragmented at first and took place mainly in smaller groups that already knew each other. These groups tried to formulate a joint operating picture and share information with the hope of being able to withstand future attacks. Unfortunately, however, the wrong information was initially spread in many cases. The greatest problem was that information did not reach the *right* people in the respective organisations *quickly enough*. Attacks started again three months later, in December 2012. Then, information sharing and cooperation among banks, internet operators, authorities and other companies worked better. The result was that this wave of attacks had virtually no effect on the banks' online services.

Lessons learned from Operation Ababil

An important lesson was that small personal/voluntary networks without any widespread support internally in the organisation don't work too well, especially in a crisis situation.

There was a certain amount of trust within groups that were used to collaborating but several actors in the rest of the financial sector had not worked and practised together before. They therefore lacked experience in cooperating. This flaw could have been rectified by collaboration exercises that include more actors and simulate different types of cyberattack.

Information sharing bodies need both strong connections *among* members as well as solid support *internally* within the respective organisations – this is to ensure that both strategic and operational information can be shared so that a joint operating picture and a joint action plan can be formulated.

Case study 2: UK cyber-exercise programme for the financial sector

In 2010, the UK Financial Supervisory Authority (FSA), in partnership with Credit Suisse, arranged an exercise to see what would happen if the country's financial sector was to come under a broad and coordinated cyberattack (Waking Shark). The aim of the exercise was to test whether the industry has a common view of how it should manage a broad cyberattack and of how communication should function effectively. Ca 100 participants from 33 financial institutions practiced together with the authorities.

One result of the exercise was the insight that there was no common view in the industry on who would take the lead in a more widespread crisis or which authority would coordinate the efforts to combat the attack. Furthermore, members of the sector's cooperation forum had no contact with internal key individuals in the field of cyber-security, which exacerbated the coordination of efforts and impaired information sharing.

The cooperation forums that were in place were not suitable to formulate a joint operating picture. The members in the cooperation forums were on a high strategic management level rather than an operational one. A parallel forum for the operative exchange of intelligence and incident information was called for in order to be able to identify the root causes of the damage more quickly and be able to combat attacks. Neither did many financial actors feel comfortable with admitting vulnerability, loss and damage in an environment where the supervisory authority was present and where competitors could benefit from the information.

The UK has several ”Information Exchanges” within the critical national infrastructure area that is to promote information exchange between private and public actors. The forum that operates within financial sector, the Financial Services Information Exchange (FSIE), was transformed into an operative group for the exchange of information in times of crisis. This transformation was then tested in the next large continuity exercise "MarketWide 2011". Here a major cyberattack was simulated in combination with a larger gas explosion in the central banking district during the London Olympics.

This exercise also showed that many financial institutions still, six months after Waking Shark, had problems to integrate business continuity, planning and cyberattack response. The FSIE forum did give the participants a better insight into the extent of the cyberattack, but participants were still on a management level. The operational cooperation needed to have its own forum. The exercise also demonstrated the importance of financial companies having a mature internal organisation where anti-cyberattack staff have the right mandate in order to be able to act quickly when needed.

Two years later the next exercise, *Waking Shark II*[21], was held. During the time between the exercises, UK authorities had built an operational cooperation platform, the Cyber Security Information Sharing Partnership (CiSP)[22]. One of the goals of Waking Shark II was to operationally test CiSP in a simulated continuity exercise and to encourage the financial sector to use the platform to a larger extent. CiSP uses a traffic-light protocol (TLP) so that members can control how information is passed on by other members. It is also possible to anonymise information, compile trends and help to spread a joint operating picture among members of CiSP.

The conclusions from Waking Shark II were that CiSP was a useful platform for operational information sharing and when a joint operating picture was desirable before, during and after a wider crisis. Membership numbers have increased significantly since the exercise.

Lessons learned from the UK cyber-exercise programme

[21] *http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf*
[22] *https://www.ncsc.gov.uk/cisp*

The UK has, similar to the US, worked to ensure that the financial sector will collaborate more than before both operationally and strategically. There are now formal agreements in place on how cooperation is to happen and what rules apply.

The UK also shows that the financial sector does not need to be subjected to a major real-life attack to be able to collaborate. Good exercises go a long way, but the cyberattacks against the US fuelled interest in cooperation. Since the same threat has not been realised in the UK, it has taken longer to foster deeper cooperation.

In both cases, the authorities have played a key role in facilitating private-public collaboration. In the UK, the supervisory authority was responsible for the main initiative.

5.4 *The work of Swedish financial authorities to promote cybersecurity*

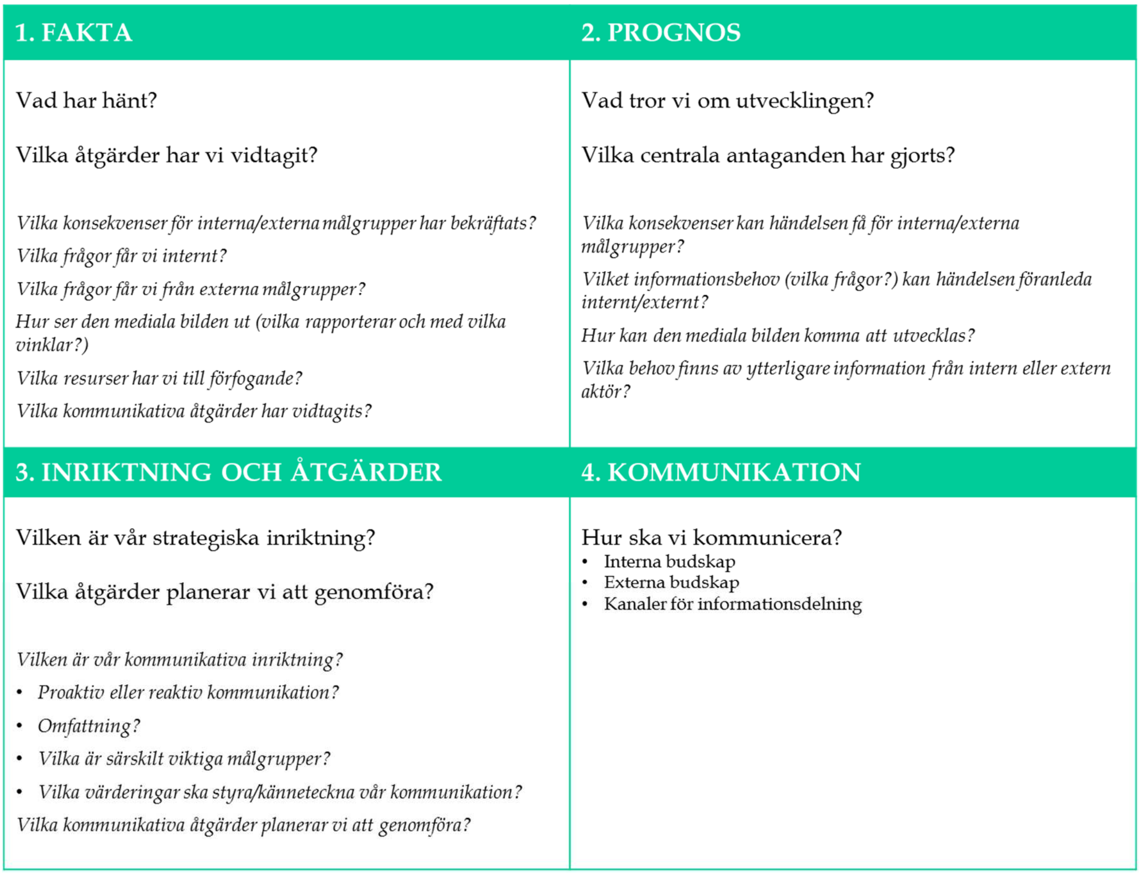
Authorities such as the Riksbank, Finansinspektionen and the National Debt Office promote financial stability and are focusing more and more on cyberattack. Issues related to financial stability are constantly analysed, risks are communicated and recommendations are put forward as to what preventive measures should be undertaken to deal with them. In addition, the sector practises both crisis prevention and crisis management. In partnership with the Ministry of Finance in the Financial Stability Council, exercises are arranged to practise crisis communication regarding various threats to financial stability.

There are also collaboration forums where there is an exchange of sensitive information and practical experience of current cyberattacks. One example is FIDIFinans, a forum for information sharing focusing on the financial sector, headed by the Swedish Civil Contingencies Agency[23]. For a full list of actors who should collaborate, see Appendix C.

[23] *MSB och samhällets informationssäkerhet (MSB and information security in society), Fact sheet January 2014, MSB.*

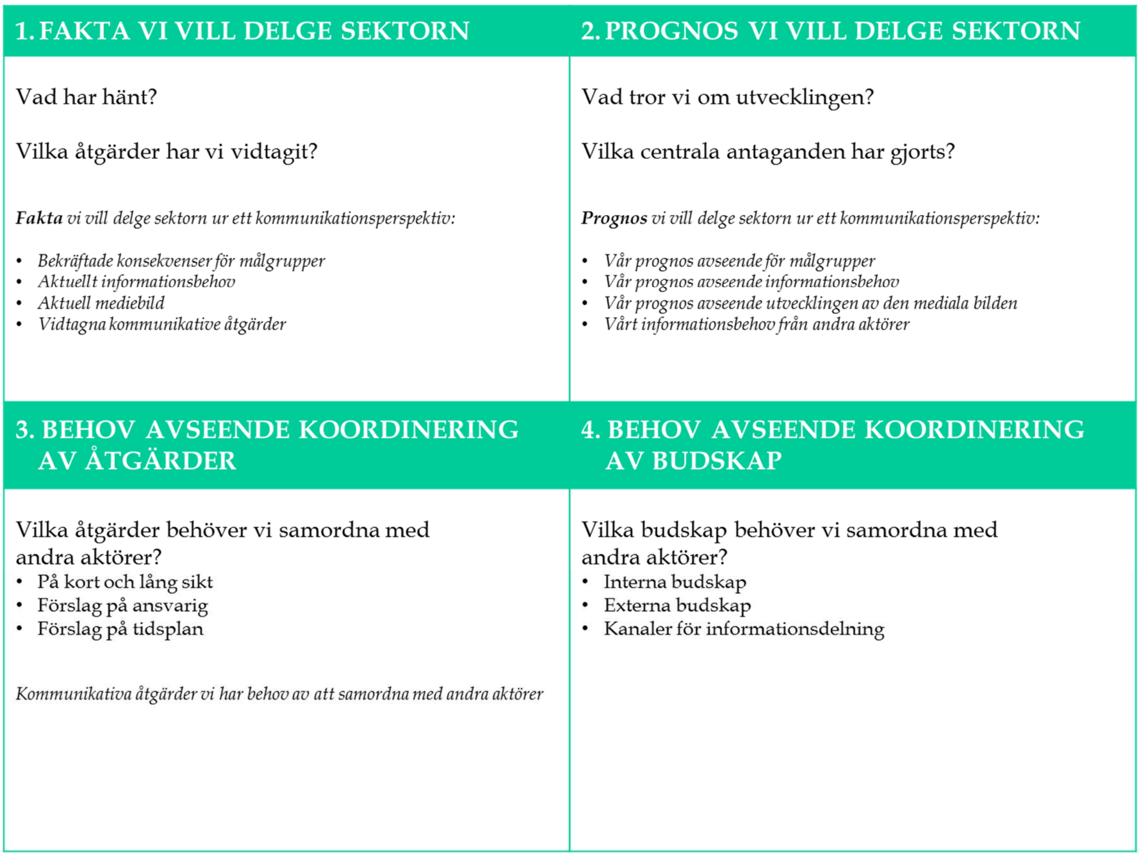
Appendix A: A foursquare for a communicational operating picture

A.1 Support questions to formulate an internal operating picture



1. FAKTA	2. PROGNOS
Vad har hänt? Vilka åtgärder har vi vidtagit? *Vilka konsekvenser för interna/externa målgrupper har bekräftats?* *Vilka frågor får vi internt?* *Vilka frågor får vi från externa målgrupper?* *Hur ser den mediala bilden ut (vilka rapporterar och med vilka vinklar?)* *Vilka resurser har vi till förfogande?* *Vilka kommunikativa åtgärder har vidtagits?*	Vad tror vi om utvecklingen? Vilka centrala antaganden har gjorts? *Vilka konsekvenser kan händelsen få för interna/externa målgrupper?* *Vilket informationsbehov (vilka frågor?) kan händelsen föranleda internt/externt?* *Hur kan den mediala bilden komma att utvecklas?* *Vilka behov finns av ytterligare information från intern eller extern aktör?*
3. INRIKTNING OCH ÅTGÄRDER	**4. KOMMUNIKATION**
Vilken är vår strategiska inriktning? Vilka åtgärder planerar vi att genomföra? *Vilken är vår kommunikativa inriktning?* • *Proaktiv eller reaktiv kommunikation?* • *Omfattning?* • *Vilka är särskilt viktiga målgrupper?* • *Vilka värderingar ska styra/känneteckna vår kommunikation?* *Vilka kommunikativa åtgärder planerar vi att genomföra?*	Hur ska vi kommunicera? • Interna budskap • Externa budskap • Kanaler för informationsdelning

A.2 Support questions to be able to share operating pictures quickly



1. FAKTA VI VILL DELGE SEKTORN	2. PROGNOS VI VILL DELGE SEKTORN
Vad har hänt? Vilka åtgärder har vi vidtagit? ***Fakta*** *vi vill delge sektorn ur ett kommunikationsperspektiv:* • *Bekräftade konsekvenser för målgrupper* • *Aktuellt informationsbehov* • *Aktuell mediebild* • *Vidtagna kommunikative åtgärder*	Vad tror vi om utvecklingen? Vilka centrala antaganden har gjorts? ***Prognos*** *vi vill delge sektorn ur ett kommunikationsperspektiv:* • *Vår prognos avseende för målgrupper* • *Vår prognos avseende informationsbehov* • *Vår prognos avseende utvecklingen av den mediala bilden* • *Vårt informationsbehov från andra aktörer*
3. BEHOV AVSEENDE KOORDINERING AV ÅTGÄRDER	**4. BEHOV AVSEENDE KOORDINERING AV BUDSKAP**
Vilka åtgärder behöver vi samordna med andra aktörer? • På kort och lång sikt • Förslag på ansvarig • Förslag på tidsplan *Kommunikativa åtgärder vi har behov av att samordna med andra aktörer*	Vilka budskap behöver vi samordna med andra aktörer? • Interna budskap • Externa budskap • Kanaler för informationsdelning

A.3 Further examples of support questions

- What do we want to achieve with our communication?
- How can our communication influence the chain of events?
- What recommendations can we include in our messages?
- What are our priority target groups and how do we reach them?
- What do our target groups' information needs look like in the short and long term?
- What measures do we need to take in order to meet these information needs?
- How is the information need influenced by implemented and planned measures to deal with the incident?
- Who is responsible for answering which questions? Need for coordination?
- Which actors do we need to coordinate our communicational measures with?

Appendix B: Working method and structure - collaboration meetings

B.1 Tips on formulating a joint communicational operating picture

The steps that should be managed and taken are found below:

- **Contact**: Effective collaboration presupposes that the actors involved can easily communicate with one another. FSPOS has an updated crisis contact list, see Appendix C for more information.

- **Meeting convener:** An invitation is sent out to those actors who should attend. The invitation shall include the time, form of collaboration conference (phone/web/video/physical), instructions for participants (for example how to call in, meeting codes, usage of mute function), purpose and agenda. The meeting convener appoints a chairman and secretary for the meeting and sees to it that documentation is created.

- **Initiate/signal need for collaboration:** The appointed authority convenes collaboration meetings but the need can be signalled by another actor. If needed, the Swedish Civil Contingencies Agency (MSB) can act as convener and host, especially when it comes to events that affect several sectors of society.

- **Meeting formats and goals**[24]: The meetings can have different goals and different formats. The most important aspect is to focus first on what the meeting is to achieve – the desired result. Only after that shall the meeting be planned, convened and held.

  Collaboration conferences can have different goals, for example to share information, establish a joint operating picture, prioritise measures or coordinate communication. A common mistake is to do too many things at each meeting. Complement therefore larger collaboration conferences with smaller work meetings with tasks that can be performed by fewer participants.

- **Leading collaboration.** The Riksbank and Finansinspektionen normally have this role in FSPOS contexts based on their respective remits, routines and technical prerequisites. The collaboration leader drives the process forward so that all the actors concerned can focus on what is most important at the time and feel confident that no-one will derive an unfair advantage from having the leading role.

[24] *See MSB Samverkanskonferenser - Råd och rekommendationer för dig som leder eller deltar i samverkanskonferenser [Collaboration conferences - Advice and recommendations for leaders and participants of collaboration conferences], section 2, pages 15-18 for examples of meetings with different goals.*

- **Meeting leader /chair**[25]: The meeting leader is responsible for preparing and leading the meeting. A meeting with many participants in a stressed situation requires clear and calm leadership as well as meticulous preparation. Difficult and controversial issues also need to be highlighted. A consensus view is not necessary, but in a stressed situation, it is an advantage if contradictory messages can be avoided as far as possible.

- **Collaboration/meeting participant:** Regarding who is invited to the meeting, it depends both on the situation and on the goal of the meeting (see reasoning above). If it is a work meeting, it is perhaps appropriate for communicators, strategists or press officers with a certain expertise to meet. A decision meeting, on the other hand, perhaps requires the presence of managers or representatives with the right mandate. Communication directors may need to agree before the sector as a whole holds a larger collaboration conference. Regardless of which, all participants must be well prepared[26].

- **Documentation**: It can be hard to remember in a stressed situation what was agreed upon. Participants in the same meeting can have a very different picture of what was said. Document therefore the result of the meeting and agreements in the simplest way possible and disseminate to the actors so that it is clear which measures will be taken and by whom.

- **Technology:** Depending on who is hosting the meeting, different technologies can be used (telephone, web, video or face-to-face meeting). The crucial aspect is not the technology itself but how easy it is to use and how accessible for all the participants.

- **Information sharing**[27]: All actors should prepare themselves to ask for information from others (be clear which information is needed and what it will be used for), create the necessary background information (find out who should have the information and whether it requires security classification), make information available for others (depending on its security classification).

B.2 Additional support

Krisinformation.se: Information from financial sectors actors is conveyed to the general public and the media on the internet and on social media. When actors in the sector have

[25] *See MSB Samverkanskonferenser - Råd och rekommendationer för dig som leder eller deltar i samverkanskonferenser [Collaboration conferences - Advice and recommendations for those leading or participating in collaboration conferences], section 4, pages 20-21 for practical advice for meeting leaders.*

[26] *See MSB Samverkanskonferenser - Råd och rekommendationer [Collaboration conferences - Advice and recommendations], section 3, page 19 for practical advice for meeting leaders.*

[27] *Gemensamma grunder för samverkan och ledning [Common basis for collaboration and leadership] - Sammanfattning [Summary], page 15.*

published verified information, the Krisinformation.se portal can help spread it to the general public and the media. Krisinformation.se is run by MSB. All information on the site has been verified by authorities and other responsible bodies.

FSPOS office: The FSPOS office regularly updates the list of contacts that actors in the financial sector use when urgent collaboration is needed.

Finanskartan.se: Finanskartan.se (The Financial Map) shows how actors in the financial sector are linked together as well as their roles and mandates in a normal situation and in a crisis situation. Please spread the word about this website to journalists.

B.3 Collaboration/work meetings for communicators within FSPOS

- Work meetings for communicators within FSPOS are held as preparation for sector-wide collaboration conferences. The aim is to prepare the joint communicational operating picture that is later part of the overall operating picture. Work meetings for communicators can produce a joint communicational operating picture that can complement an overall operating picture.

- Roles for the participating individuals can vary. Of central importance is that the representatives for the various actors bring the right background information and mandate to the meeting so that a joint communicational operating picture can be established, agreements can be reached and decisions made.

- Collaboration and work meetings can, and should sometimes, be held on different levels (managers and decision makers, strategists, communicators, web editors or press officers), depending on the goals and objectives of the meeting. Try to streamline the meeting and avoid trying to do too many things at the same time.

- Meetings are held by telephone unless otherwise decided. Work meetings can also be conducted face-to-face or with the support of other technologies.

- The convenor and host for the meeting, which can vary depending on the event, ensures that the results and conclusions are documented and shared with the meeting participants.

- For concrete tips and advice for meeting leaders and meeting participants see the MSB publication ”Samverkanskonferenser – råd och rekommendationer till dig som leder eller deltar i samverkanskonferenser [Collaboration conferences - advice and recommendations to leaders and participants of collaboration conferences][28]”.

[28] *https://www.msb.se/RibData/Filer/pdf/27251.pdf*

B.4 Agenda

Goal and objectives are updated based on the event in question.

Goal – The meeting will result in a joint communicational operating picture and an agreed overall communicational roadmap together with adopted and reconciled measures (joint as well as actor-specific).

Objective – Objective of the meeting is, based on the event in question, to create a joint communicational operating picture that will be included in the overall joint operating picture for the financial sector together with a communicational roadmap and measures that contribute to effective management.

1. The meeting is opened and a roll call is taken
2. State that a documentation officer is appointed and ready to document together with how the documentation will be distributed.
3. Present the goal and objective of the meeting (i.e. clarify the desired result)
4. Joint communicational operating picture.
    a. Each participating actor informs the sector as a whole about relevant parts of their internal operating picture that contributes to the joint communicational operating picture. (Template in appendix A)
    b. The meeting leader summarizes the joint communicational operating picture.
    c. Situation analysis and discussion if necessary.
5. The meeting leader proposes the overall roadmap for the joint communication efforts based on the operating picture and an agreement is reached.
6. Depending on the nature and development of the event, all or some of the following points are discussed:
    a. Need for common messages
    b. Need for joint communication initiatives
    c. Need of jointly reconciled questions and answers
    d. Work distribution and time plan
    e. Information about upcoming, actor-specific communication initiatives
    f. Are the information responsibilities unclear? What measures are needed?

g. Need for further analysis of target groups and channels that are specific for the event

h. Are there clear paths of contact between affected communication functions?

i. Further collaboration needs such as resources and reinforcements.

7. Summary of decisions/measures/responsibilities together with when and how feedback on implemented measures is to be given, as well as the date for the next meeting.

Appendix C – FSPOS members and roles in a crisis

This is a brief overview of actors that may need to coordinate their communication in case of a major shock in the financial sector.

NB: For contact details, you are referred to the FSPOS crisis contact list.

C.1 The Riksbank 22
C.2 Finansinspektionen 22
C.3 National Debt Office 23
C.4 Swedish Civil Contingencies Agency (MSB) 23
C.5 Banks 23
C.6 Swedish Bankers Association 24
C.7 Swedish Savings Bank Association 24
C.8 Insurance Sweden 24
C.9 Swedish Securities Dealers' Association 24
C.10 Bankgirot 24
C.11 Nasdaq 25
C.12 Euroclear 25
C.13 FSPOS 25
C.14 Ministry of Finance 26

C.1 The Riksbank

The Riksbank shall contribute to financial stability by ensuring that payments can take place securely and efficiently. The Riksbank supplies Sweden with banknotes and coins, works to prevent financial crises, have contingency and crisis management tools in place and ensures that there is a central payment system (RIX) that other economic agents can use to make payments. In a financial crisis situation, the Riksbank can also provide liquidity support to individual institutions or implement general measures to strengthen liquidity. The Riksbank also contributes overall assessments of financial stability.

C.2 Finansinspektionen (Swedish Financial Supervisory Authority)

Finansinspektionen is a central government authority tasked with ensuring the smooth running of the financial system with stable companies and a high level of consumer protection. The authority comes under the Ministry of Finance.

Finansinspektionen is responsible for supervision of financial companies and banks in Sweden and has a right to take action against companies that do not follow the legislation. Supervision can consist of ensuring that economic agents do not take greater risks than they can manage. Stress tests are a way of assessing an agent's ability to cope with external pressures, for example in a financial crisis.

In addition to the supervision responsibility, Finansinspektionen is also tasked with analysing and mitigating potential economic risks that are not associated with financial companies and, if necessary, propose measures.

Finansinspektionen shall inform the Government if it deems instability in the financial sector to be a threat to the functioning of the financial system. Finansinspektionen can get early indications about flaws in financial companies, and informs the Government if it deems possible instability to be a threat to the functioning of the Swedish financial system.

C.3 Swedish National Debt Office

The Swedish National Debt Office is central government's financial administration and plays a central role in its measures to safeguard financial stability. This role includes giving support to banks and other credit institutions in the event of a threat of a serious shock in the financial system. The Debt Office is responsible for the preparations for and management of crises in banks, other credit institutions and securities companies. It is a resolution authority, which means that it can give preventative support to organisations through guarantees, and if needed take control of institutions that are suffering problems in order to reconstruct or wind them up in a controlled manner.

The Debt Office is also responsible for the deposit guarantee, a mechanism to protect consumer savings. This protection eases concern in a financial crisis and reduces the risk of bank runs. The means to finance the support measures come from the Stability Fund, for which the National Debt Office is responsible. Banks and other credit institutions pay an annual fee to the Stability Fund.

C.4 MSB

MSB (Swedish Civil Contingencies Agency) is a central government authority responsible for supporting and coordinating accident protection efforts, crisis preparedness and civil defence. In the event of a shock, MSB shall be able to contribute support resources and ensure that those responsible coordinate their measures and their communication with the media and the general public. MSB has a supporting and coordinating role in the work on information security and cybersecurity, and is responsible for Sweden's national IT incident management function, CERT-SE.

C.5 Banks

Banks convert savings into funding, manage risks and offer payment solutions so that companies and households can save, borrow and invest. By granting credit and providing other financial services, banks create the preconditions small and medium-sized enterprises to start and grow, and for large companies to succeed in international competition.

C.6 Swedish Bankers' Association

The Swedish Bankers' Association represents Swedish banks in order to create the conditions for competitive financial products and services. Among other tasks, they disseminate knowledge about the role of banks in growth and welfare in the society.

In the event of a crisis, the Bankers' Association acts as a collaboration forum for banks, and creates the conditions for coordination between Swedish banks by, for example, organising joint conferences.

C.7 Swedish Savings Bank Association

The Swedish Savings Banks Association (Sparbankernas riksförbund) represents the Swedish savings banks, and also acts as a cooperation organisation for its members.

C.8 Swedish insurance

The basic idea of insurance companies is to create economical security for individuals and companies in relation to various kinds of risks. Policyholders pay a premier in exchange for reimbursement in case they suffer economic loss. Insurance companies manage large sums of money and are large investors in bonds, making them a significant source of investment for Swedish banks.

In contrast to banks, insurance companies cannot be affected by bank runs, although if they go bankrupt, they will not be able to make payments to claimants.

C.9 Swedish Securities Dealers' Association (SSDA)

SSDA represents common interests among companies that trade in securities in Sweden. The association currently has a membership of 29 banks and securities companies. SSDA seeks to create preconditions for a sound and efficient Swedish securities market.

It has a cooperative mission regarding issues of common interest to its members, such as the drafting of standard agreements.

C.10 Bankgirot

Bankgirot is owned by the Swedish banks and is the key player in interbank mediating retail payments in Sweden. Its system is open for all banks that have operations in Sweden. Essentially, it is a list of "addresses" that represent bank accounts and enables users to change bank accounts with no effect on use.

Bankgirot is also responsible for regulating liabilities and receivables between banks at the Riksbank regarding flows such as VISA and MasterCard, all within the framework of Bankgirot's Clearing and Settlement Service.

C.11 Nasdaq

NASDAQ OMX Stockholm AB (NASDAQ OMX) is the central marketplace for the trading of shares, premium bonds, convertibles, guarantees, bonds, exchange-traded funds, etc., in Sweden. Trade in Swedish, Finnish, Norwegian and Danish derivatives such as stock options, index options, interest rate derivatives, equity and index futures as well as certain OTC derivatives.

NASDAQ OMX Clearing Aktiebolag conducts operations concerning the clearing of derivative transactions. For these transactions, NASDAQ OMX Clearing acts as central counterparty. This means that NASDAQ OMX Clearing acts as the seller for all buyers, and the buyer for all sellers. Both the buying and selling party therefore has NASDAQ OMX Clearing as their counterparty.

C.12 Euroclear

Euroclear is both a securities depository and clearing organisation and provides services to issuers, intermediaries and investors, regarding the issue and management of financial instruments, as well as clearing and settlement of transactions.

Payments in connection of the maturity of securities and corporate actions (for example dividends) are also administrated by Euroclear. In certain cases, payment takes place in connection with settlement via central bank accounts in Euroclear and the Riksbank, and in other cases payment takes place via Bankgirot.

C.13 FSPOS

FSPOS (Finansiella Sektorns Privat-Offentliga Samverkan) is the Swedish financial sector's private-public partnership organisation and was formed on 1 September 2005. FSPOS is a voluntary collaboration forum with participants from the private business sector and public institutions in the finance sector. FSPOS vision is the constant functioning of Sweden's key financial services. Its business idea is to strengthen the financial infrastructure by collaborating, practising, analysing and sharing information, and thereby safeguard the sector and society. FSPOS members include banks, insurance companies, securities brokers, financial market infrastructures, the Swedish National Debt Office, the Riksbank and Finansinspektionen.

MSB supports the development of FSPOS; both financially, and by maintaining the FSPOS office function. FSPOS operations are led by an executive board that consists of representatives from the participating member companies and organisations.

C.14 Swedish Ministry of Finance

In the event of a crisis, the Ministry of Finance drafts proposals for measures that the Government can implement if the tools of the authorities prove insufficient. The Support to Credit Institutions Act entitles the Government to intervene with different forms of support to Swedish banks and credit institutions to prevent serious shocks in the financial system. The Ministry of Finance puts forward proposals for how such interventions should be implemented. This is in consultation with the relevant authorities. the Financial Stability Council is led by a secretariat that comes under the Ministry of Finance.

Appendix D: Reference literature (in Swedish)

- MSB (2013) Samverkanskonferenser – Råd och rekommendationer till dig som leder eller deltar i samverkanskonferenser

- MSB (2014) Gemensamma grunder för samverkan och ledning vid samhällsstörningar

- Länsstyrelsen i Västra Götalands län (2015) Kommunikationssamverkan i Västra Götalands län – Inriktning och rutiner

- Krisinformation.se (2016) www.krisinformation.se

- MSB (2016) Att stödja och samordna kommunikation. https://www.msb.se/Upload/Utbildning_och_ovning/Konferenser_seminarier/Dokumentation/Kriskommunikation_20160921/Att%20st%C3%B6dja%20och%20att%20samordna%20kriskommunikation%20med%20andra%20myndigheter%2C%20Inger%20Frendel.pdf

- Johansson, Carina (2013) Hur bedrivs framgångsrik informationssamordning? Mittuniversitetet. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyhetsarkiv/Nyhetsarkiv-2013/Hur-bedrivs-framgangsrik-informationssamordning/

- MSB (2015) Kriskommunikation vid kemikalieolyckor och oljespill i USA https://www.msb.se/sv/Start1/Kalender/Seminarium-om-amerikansk-kriskommunikation-vid-kemikalieolyckor-och-oljespill/

- MSB (Kunskapsplattform Ledning) Hur arbetar Jordbruksverket med samverkan och ledning? https://www.msb.se/Upload/Utbildning_och_ovning/Revinge/Pdf/Artikelserie%20Kunskapslpattform%20l

edning/Hur%20arbetar%20Jorbruksverket%20med%20samverkan%20och%20l
edning,%20interjvu%20med%20Catrin%20Molander,%20enhetschef.pdf