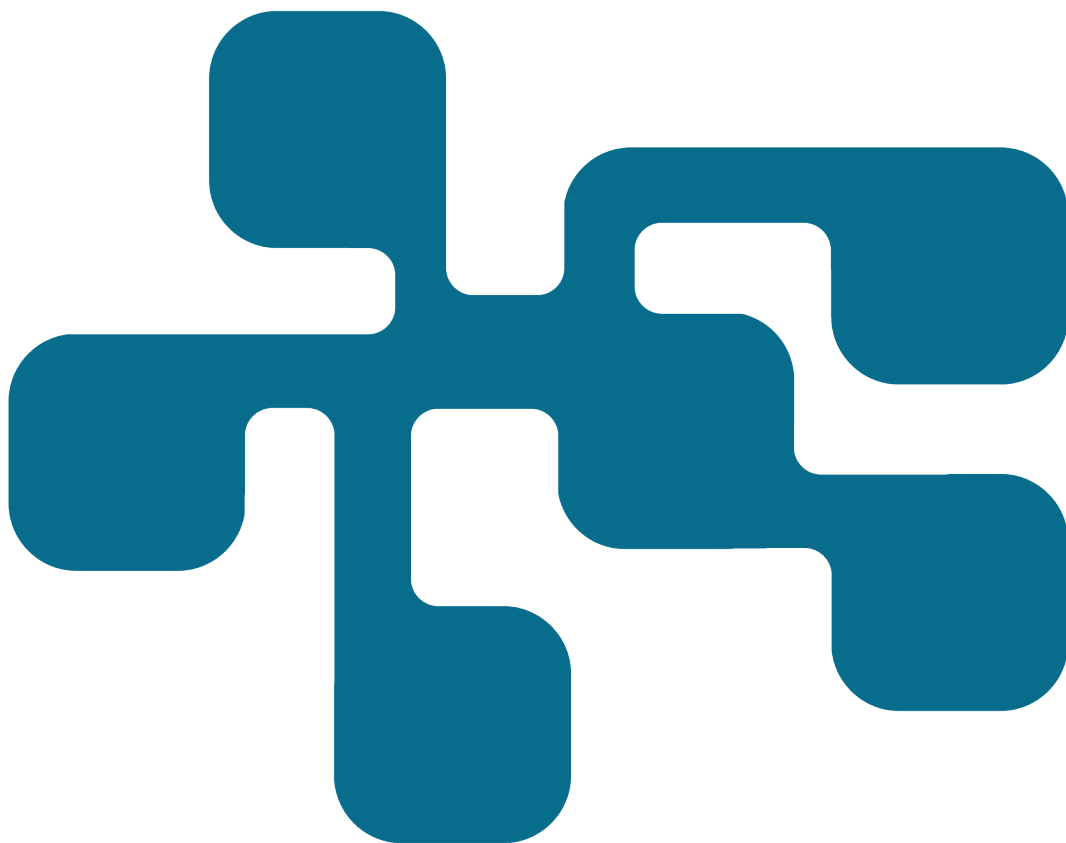


NCS3 2021

Verksamhetsrapport

Tommy Gustafsson

FOI
MSB



Tommy Gustafsson

NCS3 2021

Verksamhetsrapport

Titel	NCS3 2021 Verksamhetsrapport
Title	NCS3 2021 Annual report
Rapportnr/Report no	FOI-R--5295--SE
Månad/Month	Mars
Utgivningsår/Year	2022
Antal sidor/Pages	15
ISSN	1650-1942
Uppdragsgivare/Client	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E7160781
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett samarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Totalförsvarets forskningsinstitut (FOI) i syfte att stärka säkerheten i de system som ingår i kritisk infrastruktur. Det arbete som utförs inom NCS3 regleras via uppdrag från MSB. I denna rapport sammanfattas de uppdrag som bedrivits inom ramen för NCS3 under verksamhetsår 2021.

Under verksamhetsåret har två studier med fokus på industriella informations- och styrsystem inom hälso- och sjukvård samt hantering av elektromagnetiska hot riktade mot samhällsviktiga system genomförts. Vidare har sex kurstillfällen genomförts och en ny incidenthanteringskurs tagits fram. Arbetet har utförts av FOI:s avdelningar Försvarsanalys, Vapen, skydd och säkerhet samt Ledningssystem.

Nyckelord: NCS3, industriella informations- och styrsystem, industriella kontrollsystem, cyberfysiska system, kritisk infrastruktur, samhällsviktig verksamhet

Summary

The National Center for Security in Control Systems for Critical Infrastructure (NCS3) is a collaboration between the Swedish Civil Contingencies Agency (MSB) and the Swedish Defence Research Agency (FOI). The objective is to strengthen the security of the systems that constitute critical infrastructure. The work carried out within NCS3 is regulated by assignments from MSB. This report summarizes the assignments agreed upon during 2021.

During 2021 two studies focusing on industrial control systems in the healthcare sector and how to manage EMP-threats targeting critical infrastructure have been completed. The activities also include arranging six training courses utilizing the Swedish national cyber range Crate and development of a new incident management training course.

The assignments have been performed by the Division of Defense Analysis, the Division of Weapons, Protection and Security, and the Division of C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) at FOI.

Keywords: NCS3, industrial control systems, ICS, cyberphysical systems, critical infrastructure.

Innehållsförteckning

1	Inledning	6
1.1	Om NCS3	6
1.2	Läsanvisning.....	7
2	Medvetande-, kunskaps- och förmågehöjande verksamhet	8
2.1	Genomförande av GK-SI3S	9
2.2	Genomförande av PK-SI3S	9
2.3	Pilotgenomförande av I4S	10
3	Studier	11
3.1	Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster	11
3.2	Medicinteknik – avvikelser och CE-märkning.....	11
4	Kursutveckling	13
5	Leveranser	15

1 Inledning

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kunskapscentrum vars verksamhet genomförs i samarbete mellan Myndigheten för samhällsskydd och beredskap (MSB) och Totalförsvarets forskningsinstitut (FOI).

För verksamhetsåret finns tre överenskommelser som beskriver de uppdrag som har beställts. Dessa är *Verksamhet vid Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2021¹*, *Delbeställning: Kursverksamheter, NCS3 Studie: Incidenthantering av Elektromagnetiska hot mot samhällsviktiga tjänster²* samt *NCS3 - Medicinteknik - avvikelser och CE-märkning³*. I denna rapport sammanfattas det arbete som utförts inom NCS3 under verksamhetsår 2021.

1.1 Om NCS3

NCS3 är ett kunskapscentrum som startades år 2007 med fokus på IT-säkerhet relaterad till industriella informations- och styrsystem inom samhällsviktig verksamhet. NCS3 och dess verksamhet syftar till att minska de risker som nyttjandet av digitala system för styrning av samhällsviktig infrastruktur medför, speciellt med avseende på avsiktlig störning. Vidare syftar kunskapscentrumet till att bibehålla en hög statlig kompetens med fokus på hur industriella informations- och styrsystem används inom samhällsviktig verksamhet.

NCS3:s verksamhet ska öka säkerheten i industriella informations- och styrsystem och därigenom öka förmågan att förebygga och hantera störningar i samhällsviktig verksamhet och kritisk infrastruktur i Sverige. För att uppnå detta mål krävs ett långsiktigt arbete med fokus på:

- medvetenhet om sårbarheter, risker och möjliga åtgärder
- kompetens avseende säkerhet i industriella informations- och styrsystem
- förmåga att analysera aktuella risker och brister
- förmåga att kravställa säkerhet i industriella informations- och styrsystem.

¹ FOI-2021-339:2 samt MSB 2021-05102

² FOI-2021-261:1 samt MSB 2021-02454

³ FOI-2021-218:1 samt MSB 2021-02578

NCS3:s vision och strategi återfinns i sin helhet i dokumentet *Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017*.⁴ En ny strategi är under framtagande och kommer att publiceras under början av 2022.

De viktigaste målgrupperna för NCS3:s verksamhet är:

- aktörer som äger och driver samhällsviktig verksamhet och kritisk infrastruktur som är beroende av industriella informations- och styrsystem
- sektors- och tillsynsmyndigheter (bland annat inom Samverkansområde teknisk infrastruktur, SOTI⁵)
- myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI).

All verksamhet inom centrumet bygger på en nära samverkan mellan FOI och MSB. Samarbetet regleras genom överenskommelser vilka tas fram för varje verksamhetsår. Under 2021 har NCS3:s intresseområde utökats till att utöver mer traditionella industriella informations- och styrsystem även omfatta IoT inom samhällsviktig verksamhet. Dessa system kallas tillsammans cyberfysiska system.

1.2 Läsanvisning

I kapitel **Fel! Hittar inte referenskälla.** presenteras de utåtriktade aktiviteterna som genomförts. Exempel på utåtriktade aktiviteter är till exempel föredrag och kurser. I kapitel **Fel! Hittar inte referenskälla.** sammanfattas de studier som genomförts under året. I kapitel **Fel! Hittar inte referenskälla.** beskrivs arbetet med kursutveckling och införandet av en ny kurs. I kapitel **Fel! Hittar inte referenskälla.** återfinns en sammanställning av samtliga leveranser som har skett under verksamhetsåret.

⁴ Wedlin, M. & Hallberg, J. (2012). Vision och strategi för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet 2012 till 2017 (FOI Memo 4166).

⁵ Myndigheten för samhällsskydd och beredskap. (2016) Samverkansområdet Teknisk infrastruktur (SOTI). MSB751

2 Medvetande-, kunskaps- och förmågehöjande verksamhet

En betydande del av verksamheten inom NCS3 2021 har bestått av att ge praktiskt orienterade medvetande-, kunskaps- och förmågehöjande kurser som utvecklats och getts med hjälp av den nationella cyberanläggningen Crate. Kurserna riktar sig till beslutsfattare och tekniker som arbetar med samhällsviktiga system.

Under 2021 fanns fyra kurser som kunde ges inom ramen för NCS3. Dessa kurser var:

- *Chefskurs – Säkerhet i industriella informations- och styrsystem (CK-SI3S)*. En medvetandehöjande kurs för beslutsfattare inom verksamheter som använder industriella informations- och styrsystem för att tillhandahålla samhällsviktig verksamhet.
- *Grundläggande kurs – Säkerhet i industriella informations- och styrsystem (GK-SI3S)*. En medvetandehöjande kurs för tekniker inom verksamheter som använder industriella informations- och styrsystem för att tillhandahålla samhällsviktig verksamhet.
- *Påbyggnadskurs - Säkerhet i industriella informations- och styrsystem (PK-SI3S)*. En kunskapshöjande kurs för tekniker med fokus på säkerhetsåtgärder i miljöer med industriella informations- och styrsystem.
- *Praktisk incidenthantering i industriella informations- och styrsystem (I4S)*. En förmågehöjande kurs där tekniker får lära sig att hantera cybersäkerhetsincidenter i miljöer med industriella informations- och styrsystem.

Årets kursverksamhet påverkades av coronapandemin och genomfördes inom ramen för de generella restriktioner som utfärdats av Folkhälsomyndigheten samt de myndighetsinstruktioner som utfärdats av Regeringen. Restriktionerna och instruktionerna har varierat över tid men i princip var det endast möjligt att bedriva kursverksamheten under perioden september till december.

Samtliga kurstillfällen genomfördes under denna period och med Covid-anpassningar i enlighet med en riskanalys som genomförts av FOI. Exempel på anpassningar var att inte gå ut till en restaurang för att äta lunch, att möblera kurslokalerna så att ett avstånd på två meter kunde upprätthållas samt att tillgängliggöra handsprit och munskydd. Det skickades också ut information till kursdeltagarna om vilka Covid-anpassningar som gjorts. Utskicket innehöll en hänvisning till vid tillfället gällande rekommendationer från Folkhälsomyndigheten.

Under hela verksamhetsåret fanns begränsningar för hur stora arrangemang som fick genomföras samt begränsningar kring att resa inom landet. Detta medförde att CK-SI3S inte kunde genomföras under året då denna riktar sig mot större grupper.

2.1 Genomförande av GK-SI3S

Den 20-21 och 22-23 september genomfördes två upplagor av grundkursen. De båda tillfällena hade sammanlagt 31 deltagare, fördelade enligt Tabell 1. Deltagarnas medelbetyg för kursens innehåll och upplägg var 5,5 respektive 5,4 där 6 var bäst.

Tabell 1 Deltagare på GK-SI3S under 2021

Datum	Deltagare	Män/kvinnor
20-21 september	15	11/4
22-23 september	16	15/1

I FOI Memo 7763⁶ finns mer information om dessa kursgenomföranden samt en utvärdering baserad på deltagarnas utvärdering och lärarnas upplevelser.

2.2 Genomförande av PK-SI3S

Den 16-18 och 23-25 november genomfördes två upplagor av Påbyggnadskurs: Säkerhet i industriella informations- och styrsystem. De båda kurserna hade sammanlagt 26 deltagare, fördelade enligt Tabell 2. Att samtliga 16 kursplatser inte utnyttjades berodde på att flera deltagare fick avboka kursen med kort varsel till följd av gällande Covid-restriktioner. Deltagarnas medelbetyg för kursens innehåll, relevans och upplägg var 6,1 på en sju-gradig skala för båda kurserna.

Tabell 2 Deltagare på GK-SI3S under 2021

Datum	Deltagare	Män/kvinnor
16-18 november	13	10/3
23-25 november	13	12/1

I FOI Memo 7791⁷ finns mer information om dessa kursgenomföranden samt en utvärdering baserad på deltagarnas utvärdering och lärarnas upplevelser.

⁶ Valassi, C. & Gustafsson, T. (2021). Kursutvärdering – Grundläggande kurs SI3S (GK-SI3S) september 2021 (FOI Memo 7763).

⁷ Valassi, C. & Gustafsson, T. (2021). Kursutvärdering – påbyggnadskurs Säkerhet i industriella informations- och styrsystem (PK-SI3S) – november 2021 (FOI Memo 7791).

2.3 Pilotgenomförande av I4S

Den 18-21 och 25-28 oktober genomfördes två pilotupplagor av Praktisk incidenthantering i industriella informations- och styrsystem. Dessa genomföranden var de första gångerna som den nyutvecklade versionen av I4S genomfördes, se kapitel 4. De båda kurserna hade sammanlagt 27 deltagare, fördelade enligt Tabell 3. Återigen var kursen inte fullbokad, vilket berodde på att flera deltagare fick avboka sig med kort varsel. Deltagarnas medelbetyg för kursens innehåll, relevans och upplägg var 6,0 respektive 5,9 på en sju-gradig skala. Av utvärderingen framgår att kursens praktiska moment i Crate var särskilt uppskattade av deltagarna med betyg på 6,3 respektive 6,4.

Tabell 3 Deltagare på GK-SI3S under 2021

Datum	Deltagare	Män/kvinnor
18-21 oktober	13	12/1
25-28 oktober	14	13/1

I FOI Memo 7764⁸ finns mer information om dessa kursgenomföranden samt en utvärdering baserad på deltagarnas utvärdering och lärarnas upplevelser.

⁸ Valassi, C. & Gustafsson, T. (2021). Kursutvärdering – Praktisk incidenthantering i industriella informations- och styrsystem (I4S) – oktober 2021 (FOI Memo 7764).

3 Studier

Inom NCS3 genomförs studier i syfte att bättre förstå den miljö där industriella informations- och styrsystem används men även för att studera hur en teknik eller process kan tillämpas inom området. På en övergripande nivå delas studierna in i sektorstudier där användandet av industriella informations- och styrsystem inom en viss sektor studeras samt tekniska studier där tekniska och administrativa säkerhetsåtgärder studeras. Under år 2021 genomfördes två tekniska studier.

3.1 Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster

Inom projektet *NCS3 Studie: Incidenthantering av Elektromagnetiska hot mot samhällsviktiga tjänster*⁹ utarbetades en vägledning med fokus på elektromagnetiska hot. Vägledningen finns publicerad i form av ett FOI-memo¹⁰ och beskriver dels hur en pågående incident kan hanteras, dels vilka åtgärder som kan vidtas för att förhindra incidenter. Vägledningen bygger på studier som FOI tidigare har genomfört på uppdrag av MSB och listar ett antal generella åtgärds punkter som kan anpassas beroende på den verksamhet man vill skydda.

3.2 Medicinteknik – avvikelser och CE-märkning

Inom projektet *NCS3 Medicinteknik – avvikelser och CE-märkning*¹¹ genomfördes en intervjustudie med fokus på hur vårdgivare, företag och myndigheter arbetar med cybersäkerhet rörande medicintekniska produkter. Studien är en fortsättning på en flerårig studieverksamhet med fokus på medicintekniska produkter som har genomförts inom ramen för NCS3. Studien finns publicerad i en FOI-rapport¹². I rapporten beskrivs hur personal inom hälso- och sjukvård arbetar med avvikelserapportering samt hur regelverk och certifieringsmöjligheter förhåller sig till patientsäkerhet och cybersäkerhet. Slutsatser av studien som lyfts fram i rapporten är bland annat att medicinteknisk personal behöver samverka med informationssäkerhets- och IT-

⁹ FOI-2021-261:1 samt MSB 2021-02454

¹⁰ Nyholm, S., Wiklund, K. & Hurtig, T. (2021). Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster (FOI Memo 7507).

¹¹ FOI-2021-218:1 samt MSB 2021-02578

¹² Wahrenberg, J., Stenerus, A-S., Mittermaier, E., Eckersand, U. (2022). Patient- och cybersäkerhet rörande medicinteknisk utrustning. En NCS3-studie om avvikelshantering och CE-märkning. FOI-R--5226--SE.

säkerhetsavdelningar. Vidare finns det ett stort behov av personal med kompetens inom cybersäkerhet, patientsäkerhet samt regelverk och certifieringsarbete hos tillverkare och vårdgivare. Även avvikelserapporteringen med fokus på cyberrelaterade avvikelser behöver förbättras.

4 Kursutveckling

Under 2020 och 2021 tog FOI på uppdrag¹³ av MSB fram en ny version av kursen *Praktisk incidenthantering för industriella informations- och styrsystem* (I4S). Inför utvecklingsarbetet gjordes en förstudie där bristerna i den tidigare kursen samt förslag på åtgärder identifierades i dialog med MSB.

Följande brister identifierades i den föregående kursen:

- Deltagarna fick begränsad kunskap om metoder för incidenthantering.
- Den tidigare kursen avslutades med ett övningspass som pågick en hel dag vilket upplevdes för krävande och för långt.
- Under övningarna arbetade deltagarna i två lag med åtta personer per lag. De stora grupperna gjorde att flera deltagare blev passiva då de hade svårt att hitta uppgifter.
- Den emulerade övningsmiljön¹⁴ upplevdes för obekant.
- Den emulerade övningsmiljön och de inspel som användes upplevdes föråldrade då dessa var från 2013.

Utvecklingsarbetet skedde i enlighet med en plan som togs fram i samråd mellan FOI och MSB¹⁵ och den nya kursen finns beskriven i FOI Memo 7810¹⁶. Som beskrevs i Avsnitt 2.3 gavs två pilotgenomföranden av kursen i oktober 2021. Dessa var framgångsrika även om ett antal förbättringsbehov identifierades, framförallt med fokus på laborationer och stabilisering av den emulerade övningsmiljön samt de inspel som skedde under kursen. Både pilotgenomförandena och förbättringsbehoven beskrivs närmare i FOI Memo 7764¹⁷.

Utvecklingen av den emulerade övningsmiljön i Crate samordnades med projekten *Förstudie Threat hunting i CRATE*¹⁸ och *Crate – Övningsmoduler och*

¹³ Verksamhet vid Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) 2021, (dnr FOI-2021-339, MSB 2021- 05102)

¹⁴ Med emulerad övningsmiljö avses en övningsmiljö som med hjälp av virtualisering har byggts upp i cyberanläggningen Crate.

¹⁵ Westerdahl, L. (2020). Planerad utveckling av NCS3-kursen I4S 2020 (FOI Memo 7200).

¹⁶ Gustafsson, T. (2022). NCS3 Kursutveckling – Praktisk incidenthantering i industriella informations- och styrsystem (FOI Memo 7810)

¹⁷ Valassi, C. & Gustafsson, T. (2021). Kursutvärdering – Praktisk incidenthantering i industriella informations- och styrsystem (I4S) – oktober 2021 (FOI Memo 7764).

¹⁸ FOI-2020-797:3 samt MSB 2020-07809

*onlineföreläsningar*¹⁹. Utvecklingen samordnades också med det utvecklingsarbete av cyberanläggningen som skedde inom projektet *Nationell cyber range CRATE 2.0*²⁰. Samordningarna har både medfört kostnadsbesparingar och gjort det möjligt att bygga en mer avancerad övningsmiljö. Vidare har nyttjandet av nya funktioner och verktyg i Crate gjort det möjligt att förenkla och automatisera både skapandet av multipla emulerade övningsmiljöer och genomförandet av kursens tre övningspass.

¹⁹ FOI-2021-431:4 samt MSB 2021-02352

²⁰ FOI-2016-836:2 samt MSB 2016-1122

5 Leveranser

I Tabell 4 presenteras de skriftliga leveranser som har skett inom ramen för NCS3 verksamhetsår 2021.

Tabell 4: Skriftliga leveranser som har publicerats inom NCS3 under verksamhetsår 2021.

Referens	Titel	Överenskommelse
FOI Memo 7507	Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster	MSB 2021-02454
FOI Memo 7763	Kursutvärdering - Grundläggande kurs SI3S (GK-SI3S) september 2021	MSB 2021-05102
FOI Memo 7764	Kursutvärdering – Praktisk incidenthantering i industriella informations- och styrsystem (I4S)	MSB 2021-05102
FOI Memo 7791	Kursutvärdering - Påbyggnadskurs SI3S (PK-SI3S) november 2021	MSB 2021-05102
FOI Memo 7810	NCS3 Kursutveckling - Praktisk incidenthantering i industriella informations- och styrsystem (I4S) 2021	MSB 2021-05102
FOI-R--5226--SE	Patient- och cybersäkerhet rörande medicintekniska produkter - En NCS3-studie om avvikelshantering och CE-märkning	MSB 2021-02578
FOI-R--5295--SE	NCS3 2021 Verksamhetsrapport	MSB 2021-05102



Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.



FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se



Swedish Civil
Contingencies
Agency

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se