Ekonomisk kommentar

En cyberattack kan påverka den finansiella stabiliteten

Lukas Elestedt, Ulrika Nilsson och

Carl-Johan Rosenvinge

NR 8 2021, 19 maj

Innehållsförteckning

1	Inledning	4
2	Vad är cyberrisk?	5
2.1	Cyberrisk skiljer sig från traditionella operativa risker	6
3	En cyberattack kan påverka den finansiella stabiliteten	7
4	Förståelse för hotbilden är central för att hantera cyberrisk	12
5	Avslutande kommentarer	16
	Referenser	17

Ekonomiska kommentarer

Ekonomiska kommentarer är korta analyser om relevanta frågor för Riksbanken. Den kan författas av både enskilda direktionsledamöter och medarbetare på Riksbanken. Medarbetares kommentarer godkänns av avdelningschef medan direktionsledamöterna själva ansvarar för innehållet i sina kommentarer.

Sammanfattning

Lukas Elestedt, Ulrika Nilsson och Carl-Johan Rosenvinge
Författarna är verksamma vid avdelningen för finansiell stabilitet.

När den finansiella sektorn blir allt mer digitaliserad ökar sårbarheterna för cyberattacker. Denna utveckling sker samtidigt som de kvalificerade cyberattackerna ökar och sammantaget innebär detta att cyberrisker för den finansiella sektorn ökar. Cyberrisk skiljer sig från andra operativa risker, bland annat genom att cyberattacker kan komma från hotaktörer med ont uppsåt. Cyberrisk karakteriseras också av snabbhet och skalbarhet, där en cyberattack har potential att snabbt nå mycket stor spridning.

Slutsatsen av denna analys är att en cyberattack kan påverka den finansiella stabiliteten, och att cyberrisk därmed utgör en systemrisk. I analysen beskrivs hur en cyberattack mot finansiell sektor eller dess kritiska tjänsteleverantörer direkt kan påverka finansiell stabilitet, om den eller de aktörer som drabbas är tillräckligt kritiska och attackens konsekvenser tillräckligt allvarliga. Även i de fall där den direkta påverkan av attacken är begränsad finns en risk att attackens konsekvenser får negativa följdeffekter som förvärras och sprids vidare i det finansiella systemet, exempelvis i form av bristande förtroende för systemet.

För att kunna begränsa cyberrisken i det finansiella systemet är det avgörande att varje aktör har förståelse för både vad som behöver skyddas och mot vad det behöver skyddas. Åtgärder som syftar till att förebygga och stoppa cyberattacker behöver kompletteras med en förmåga att upptäcka, avfärda och återhämta sig från dem. För att förbättra motståndskraften är god samordning mellan myndigheter och finansiell sektor och en långsiktig planering för minskad sårbarhet för det finansiella systemet viktigt.

Författarna vill tacka Johanna Stenkula von Rosen, Kristian Jönsson, Olof Sandstedt, Caroline Jungner och Kevin Aytap för värdefulla synpunkter. De åsikter som uttrycks i denna ekonomiska kommentar är författarnas egna och ska inte uppfattas som Riksbankens syn i dessa frågor.

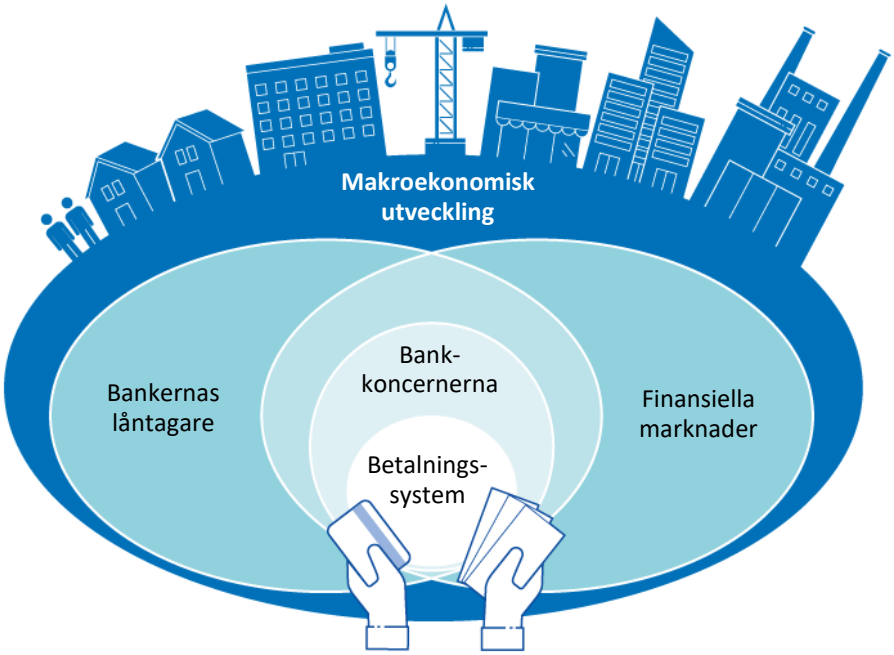
---

1 Inledning

Cyberattacker får mer och mer uppmärksamhet i samhället. Dessa attacker har potential att påverka myndigheter och företag såväl som privatpersoner. Den finansiella sektorn är inget undantag. Enligt BIS utsätts den finansiella sektorn för ett större antal cyberattacker än andra sektorer.[1]

Den finansiella sektorn utgörs av aktörer som verkar inom det finansiella systemet. Till dem räknas till exempel banker och infrastrukturföretag vars funktioner är avgörande för att det finansiella systemet, och i förlängningen Sveriges ekonomi, ska fungera. I och med att finansiella företag har en särskild funktion och en särskild ställning regleras de i en särskild ordning.[2] Ett sätt att övergripande illustrera det finansiella systemets uppbyggnad och dess vikt för en stabil makroekonomisk utveckling är enligt Figur 1 nedan.

Figur 1. Illustration av det finansiella systemets uppbyggnad



Källa: Sveriges riksbank.

I det finansiella systemets centrum finns betalningssystem och andra finansiella infrastrukturföretag. Dessa är tätt sammanlänkade med bankerna, och tillsammans bygger de upp kärnan i det finansiella systemet. Den finansiella infrastrukturen och bankerna utgör en bas för fungerande finansiella marknader och tillräcklig kredittillgång i systemet. För en fungerande ekonomi behöver det finansiella systemet utföra en lång rad ekonomiska nyckelfunktioner, så kallade kritiska funktioner, på ett pålitligt och

[1] Se I. Aldasoro, L. Gambacorta, P. Giudici och T. Leach (2020), The drivers of cyber risk, *BIS Working Papers No 865*. Bank for International Settlements.

[2] Se *Riksbanken och finansiell stabilitet*, februari 2013. Sveriges riksbank.

robust sätt.[3] Detta inkluderar till exempel att tillhandahålla tjänster relaterade till sådant som betalningar och avveckling, interbanklån, transaktions- och sparkonton samt derivat- och värdepappershandel. I slutändan är ett fungerande finansiellt system därför en förutsättning för en stabil makroekonomisk utveckling.

I dag upprätthålls det svenska finansiella systemets kritiska funktioner nästintill uteslutande på digital väg. Den långtgående digitaliseringen har medfört att banker och finansiella infrastrukturföretag i dag är helt beroende av sina IT-miljöer för att tillhandahålla tjänster. Samtidigt har dessa miljöer vuxit snabbt och blivit allt mer sammanlänkade och komplexa. Detta gäller bankernas och infrastrukturföretagens IT-system, men även deras tredjepartsleverantörer och teknisk infrastruktur som telekommunikation och energiförsörjning.[4] Denna utveckling innebär ökade sårbarheter för det finansiella systemet och har dessutom skett i kombination med att hotbilden har breddats och kvalificerade cyberattacker ökar.[5]

I den här publikationen illustrerar vi hur en cyberattack skulle kunna leda till finansiell instabilitet. Vi beskriver även vad cyberrisk är och hur den skiljer sig från andra risker, vikten av att förstå hotbilden för att adekvat kunna hantera cyberrisk, vilken roll staten har och behovet av samordning och samarbete mellan myndigheter och finansiell sektor.

2 Vad är cyberrisk?

Cyberrisk definieras av Financial Stability Board (FSB) som kombinationen av sannolikhet för och konsekvenserna av cyberincidenter. En cyberincident är en händelse i ett informationssystem som äventyrar säkerheten i informationssystemet eller bryter mot säkerhetspolicyer, oavsett om det sker med ont uppsåt eller inte.[6] Begreppet risk skiljer sig här från när man till exempel talar om företag i den finansiella sektorn som aktivt tar risker för att få en högre avkastning. Detta rör finansiella risker som exempelvis kan handla om likviditetsrisk, marknadsrisk eller kreditrisk. Men finansiella företag utsätts även för operativa risker, som till skillnad från finansiella risker inte är en direkt följd av en avvägning mellan risk och förväntad avkastning. En operativ risk kan definieras som risken för förluster, störningar, avbrott eller skadat anseende från otillräckliga eller misslyckade interna processer, människor, system eller externa händelser.[7] Cyberrisk kan ses som en del av operativ risk, men har ofta vissa särdrag som skiljer den från mer traditionella operativa risker.

[3] Se exempelvis Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag.

[4] Se exempelvis *Finansiell stabilitet*, juni 2016. Sveriges riksbank. och F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden.

[5] Se *FRA årsrapport 2020*, mars 2021. Försvarets radioanstalt. och *FRA årsrapport 2018*, januari 2019. Försvarets radioanstalt.

[6] Se *FSB Cyber Lexicon*, november 2018. Financial Stability Board.

[7] Se exempelvis *Principles for Financial Market Infrastructures*, april 2012. Bank for International Settlements och International Organization of Securities Commissions. och *Principles for the Sound Management of Operational Risk*, juni 2011. Bank for International Settlements.

Normalt sett använder Riksbanken FSB:s definition av cyberrisk. Men för att förenkla analysen i denna ekonomiska kommentar kommer vi istället använda begreppet cyberrisk för den del av incidenterna som utgörs av ett angrepp initierat av aktörer med ont uppsåt.

2.1 Cyberrisk skiljer sig från traditionella operativa risker

Hotet från antagonistiska aktörer innebär en väsentlig skillnad mellan cyberrisk och andra operativa risker (förutom traditionella bedrägeririsker) som finansiella företag står inför. Utöver detta karakteriseras cyberrisk av två andra aspekter[8]: snabbhet och skalbarhet. Med snabbhet avses att en cyberattack kan spridas mycket snabbt genom drabbade IT-miljöer. I många fall kan attacken vara designad för just detta. Med skalbarhet avses att många olika företag runt om i världen använder liknande hård- och mjukvara, och en cyberattack har därmed potential att nå mycket stor spridning. Detta kan vara avsiktligt men även oavsiktligt. Ett exempel på detta, utanför den finansiella sektorn, är cyberattacken NotPetya[9] som 2017 drabbade en långt större krets än vad som ursprungligen bedömts vara avsikten. Exempelvis drabbades det danska rederiet Maersk mycket hårt, trots att de sannolikt inte var målet för attacken.[10]

Det är svårt att få tillförlitlig statistik om cyberattacker

Det finns sannolikt stora mörkertal kring cyberrisk, vilket gör det svårt att ta fram statistik för att kunna beräkna den. Den finansiella sektorn är överlag van vid god tillgång till data för att kunna beräkna risker. Men när det gäller cyberrisk är bristen på tillförlitlig data ett problem, speciellt på sektornivå. Problemen med att kvantifiera cyberrisk beror till stor del på att drabbade företag har svaga incitament för att rapportera allvarliga cyberincidenter till myndigheter, ägare och andra intressenter. Det finns nämligen en risk i sig med att vara öppen och informera om det. Samtidigt är det positivt för samhället i stort om fler incidenter rapporteras så att statistiken och kunskapsläget förbättras. Statistikinsamlingen försvåras ytterligare av att de kvalificerade intrången, och därmed också de mest relevanta, i många fall de som är svårast att upptäcka.

För att hantera problemet med bristande data försöker man i allmänhet basera analyser på de delar av data som man har störst förtroende för. Det leder bland annat till att ett vanligt mått på cyberrisk är antalet intrång.[11] Utifrån ett systemriskperspektiv är detta dock ett bristfälligt mått eftersom det är intrångets potentiella konsekvenser

[8] Se bland annat *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

[9] NotPetya är en så kallad kryptomask som började spridas 2017 och som genom kryptering av kritiska filer bland annat förhindrade användaren att starta operativsystemet.

[10] Se T. Gustafsson och D. Lindahl (2019), Cyberförsvar – färdighet kräver övning, *FOI Memo 6747*. Totalförsvarets forskningsinstitut. och E. Zouave och M. Jaitner (2019), Säkra leverantörskedjor för styrsystem, *FOI-R—4759*. Totalförsvarets forskningsinstitut.

[11] Se F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden. för en diskussion kring hur kvalitet och tillgänglighet av data för cyberattacker kan förbättras.

som är av störst vikt. Denna typ av mått blir också mycket känsligt för hur man väljer att definiera vad en cyberattack är. Cyberattacker kan vara osofistikerade och mer eller mindre automatiserade försök att få tillgång till en organisations system, men även mer kvalificerade och framgångsrika i att exempelvis slå ut en organisations kritiska funktioner. En cyberattack kan med andra ord skilja sig mycket från en annan, dels vad gäller inriktning och tillvägagångssätt och dels vad gäller de konsekvenser den orsakar. Denna skillnad gör att definitioner blir viktiga.

Ovan beskrivna problem med statistik påverkar naturligtvis inte risken i sig direkt. Däremot innebär det att risken blir svårare att följa och det påverkar möjligheterna att fatta lämpliga beslut, vilket potentiellt kan påverka sårbarheterna och därmed indirekt risken.

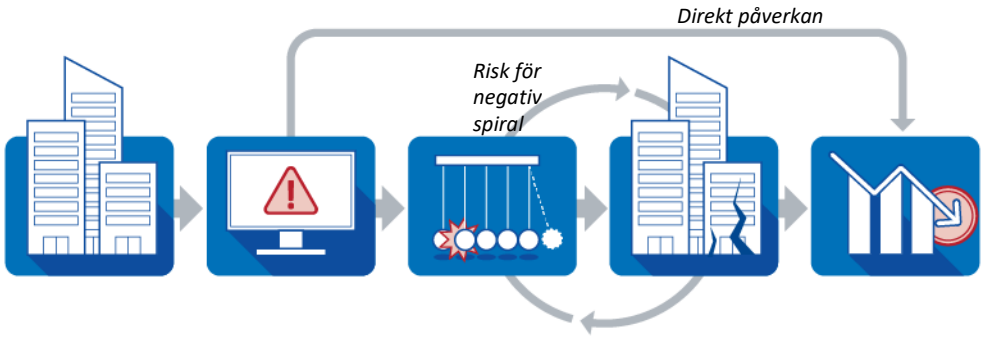
3 En cyberattack kan påverka den finansiella stabiliteten

Med cyberrisk menar vi alltså i den här publikationen en kombination av sannolikheten för och konsekvenserna av att en händelse med antagonistiskt ursprung äventyrar säkerheten i en organisations informationssystem. I och med att cyberattacker kan påverka aktörer på de finansiella marknaderna kan de också potentiellt påverka den finansiella stabiliteten och utgöra en systemrisk.[12] Med tanke på hur viktigt det finansiella systemet är för samhällsekonomin kan en cyberattack mot den finansiella sektorn i förlängningen utgöra ett hot mot en fungerande ekonomi.

I Figur 2 nedan illustrerar vi hur man kan dela upp en cyberattack i fem olika skeden: attackens mål, attackens direkta påverkan, attackens potentiella spridningseffekter, attackens indirekta påverkan samt attackens samlade påverkan på finansiell stabilitet. Ur ett finansiellt stabilitetsperspektiv kan man säga att en cyberattack börjar då någon eller några aktörer drabbas av den. Dessa kan antingen vara finansiella aktörer eller tredjepartsleverantörer till den finansiella sektorn. Nästa aspekt är direkt påverkan, det vill säga hur dessa aktörer påverkas av attacken genom att exempelvis tillgängligheten till vissa tjänster brister. Därefter kan dessa effekter spridas vidare i det finansiella systemet, vilket i sin tur indirekt kan påverka antingen samma aktör ytterligare eller andra. Det sista steget är att den här påverkan på enskilda aktörer blir så stor att även den finansiella stabiliteten påverkas.

[12] Systemrisk innebär en risk för störning i det finansiella systemet med potential att få allvarliga negativa följder för den reala ekonomin, se exempelvis *Riksbanken och finansiell stabilitet*, februari 2013. Sveriges riksbank. eller *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

Figur 2. Hur en cyberattack kan påverka den finansiella stabiliteten



Attackens mål
- Systemviktigt finansiellt företag
- Flera finansiella företag
- Tredjeparts-leverantör till finansiell sektor

Direkt påverkan
- Konfidentialitet
- Riktighet
- Tillgänglighet

Potentiella spridnings-effekter
- Förtroende
- Operationellt
- Finansiellt

Indirekt påverkan
- Direkt påverkan
- Samt:
  - Finansiella förluster
  - Förtroende
  - Risk för negativ spiral

Påverkan på finansiell stabilitet

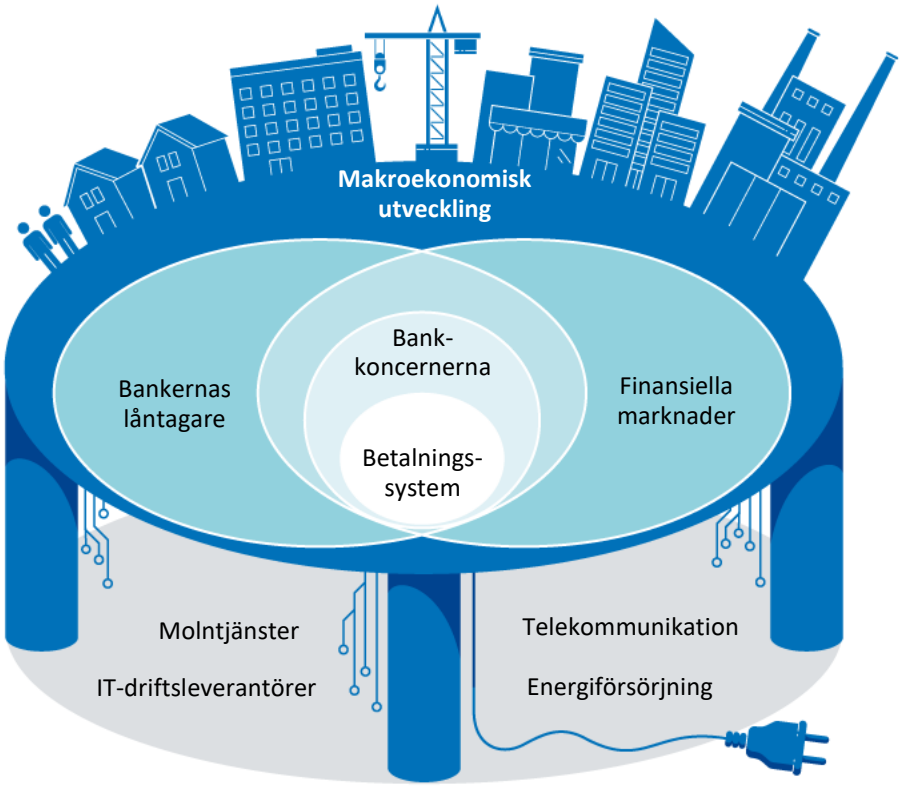
Källa: Europeiska systemrisknämnden, Internationella valutafonden och Sveriges riksbank.

1. Attackens mål – startpunkten för cyberattacken

När man analyserar en cyberattack ur ett finansiellt stabilitetsperspektiv kan man se det som att en attack börjar med att någon eller några aktörer drabbas av den, se *attackens mål* i Figur 2. Cyberattacken riktas initialt mot *ett* systemviktigt finansiellt företag, *flera* finansiella företag eller mot en tredjepartsleverantör till den finansiella sektorn.[13] Med tredjepartsleverantör till finansiell sektor avses till exempel sådant som rör IT-drift, mjukvara, molntjänster, energiförsörjning och kommunikation. För att täcka in detta i den schematiska bilden i Figur 1 måste vi utöka den, så att även tredjepartsleverantörers tjänster räknas in som kritiska tjänster som understödjer det finansiella systemets funktioner och i slutändan makroekonomin, se Figur 3 nedan.

[13] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

Figur 3. Kritiska tjänster understödjer det finansiella systemets funktioner



Källa: Sveriges riksbank.

2. Direkt påverkan – initiala konsekvenser av cyberattacken

Nästa steg är hur en eller flera aktörer som drabbats av en cyberattack påverkas av den, se *direkt påverkan* i Figur 2. Här avser vi vilken teknisk och verksamhetsmässig påverkan en cyberattack kan få initialt. Detta skede handlar alltså om konsekvenserna av en cyberattack och inte sannolikheten för en.

Som nämnts i inledningen utför det finansiella systemet ett antal kritiska funktioner. Det är stora värden som rör sig genom det svenska finansiella systemet varje dag, vilket gör systemet sårbart för störningar. Exempelvis omsätts dagligen cirka 670 miljarder kronor i Riksbankens centrala betalningssystem för stora betalningar, RIX.[14] För att utföra sina kritiska funktioner förlitar sig det finansiella systemet på robust informations- och kommunikationsteknologi.

Vidare så är det finansiella systemet beroende av kritisk information i dessa system, som behöver skyddas. Konfidentialitet, riktighet och tillgänglighet (även benämnt CIA[15]) är tre centrala aspekter som ständigt återkommer när det handlar om cybersäkerhet och att skydda information. De kan definieras enligt följande:

[14] Se Sveriges riksbank, *Betalningssystemet RIX*, senast uppdaterad 5 mars 2021. Hämtad 8 maj 2021 https://www.riksbank.se/sv/betalningar--kontanter/betalningssystemet-rix/

[15] CIA – förkortning av Confidentiality, Integrity, Availability.

- Konfidentialitet: att bevara informationens sekretess och förhindra att information kommer obehöriga till del
- Riktighet: att bevara informationens korrekthet och förhindra att den olovligen förändras eller manipuleras
- Tillgänglighet: att bevara åtkomst till informationen för behöriga och förhindra att den förstörs eller på annat sätt görs otillgänglig[16]

Utifrån ett finansiellt stabilitetsperspektiv, och även ur den enskilda aktörens perspektiv, är en av de mest kritiska aspekterna att verksamheten kan fortgå. Därmed är betydelsen av att upprätthålla tillgängligheten central. Det kan dock i vissa fall vara värre att låta en verksamhet fortgå om en eller flera finansiella verksamheters information har manipulerats. Riktighetsaspekten är därför även den central att upprätthålla.[17] Även om konfidentialiteten påverkas på ett omfattande sätt kan det inverka negativt på systemnivå. Ett flertal vanliga typer av cyberattacker påverkar såväl tillgänglighets- som riktighetsaspekter hos den drabbade aktören. Ofta innebär en cyberattack att flera, och ibland samtliga, av dessa aspekter påverkas i en och samma attack. För företag och privatpersoner skulle det kunna ta sig uttryck på många olika sätt, beroende på attackens syfte, mål och tillvägagångssätt, till exempel genom problem med att komma åt internet- eller mobilbank, felaktiga saldouppgifter, felaktiga ägaruppgifter för värdepapper eller problem med att genomföra transaktioner.

Hur stor påverkan en cyberattack får kan också se olika ut beroende på vilken aktör som drabbas. Om det till exempel enbart finns en eller ett fåtal aktörer som erbjuder vissa kritiska funktioner kan en cyberattack mot dessa leda till att en viktig funktion inte går att upprätthålla alls. Detta innebär att *bristande utbytbarhet* där det saknas alternativ till vissa tjänster, som det centrala betalningssystemet för stora betalningar[18], kan påverka den finansiella stabiliteten. Störningar hos denna kritiska funktion skulle i sin tur kunna leda till följdeffekter i en stor del av det finansiella systemet.[19]

3. Potentiella spridningseffekter – hur attackens konsekvenser kan spridas och förstärkas

Efter attackens initiala påverkan kan effekterna av den sprida sig vidare eller förstärkas, se *potentiella spridningseffekter* i Figur 2. I fallet NotPetya, som nämnts ovan, skedde spridningen snabbt och i stor skala. Effekterna drabbade cirka 10 procent av Ukrainas datorer och spreds även långt utanför landets gränser.[20]

[16] Se exempelvis *Vägledning i säkerhetsskydd, Informationssäkerhet*, september 2020. Säkerhetspolisen.

[17] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

[18] För det svenska finansiella systemet motsvaras detta av Riksbankens betalningssystem, RIX.

[19] Se F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden.

[20] Se T. Gustafsson och D. Lindahl (2019), Cyberförsvar – färdighet kräver övning, *FOI Memo 6747*. Totalförsvarets forskningsinstitut.

Här beskriver vi tre olika kanaler genom vilka chocken från en cyberattack kan förstärkas eller spridas till fler aktörer.[21] Den första är *förtroendekanalen*. Det innebär att en cyberattack kan leda till bristande förtroende för den aktör som är utsatt, men även för andra liknande aktörer såväl som för det finansiella systemet i stort. Hur stora förtroendeeffekterna blir beror bland annat på det finansiella systemets grundtillstånd, hur allvarliga konsekvenserna av attacken är, hur länge aktören eller aktörerna påverkas samt hur många aktörer som påverkas av attacken.[22] Det är viktigt att finansiella marknader, företag och allmänheten har förtroende för det finansiella systemet. Om man tappar i förtroende kan det i förlängningen leda till en uttagsanstormning mot banker eller andra finansiella företag och den finansiella stabiliteten kan hotas.

Den andra är den *operationella kanalen*. Det finansiella systemet är tätt sammanlänkat både på det finansiella och på det tekniska planet. Detta leder till att operationella problem hos en aktör kan spridas vidare till andra aktörer. På det finansiella planet är olika centrala aktörer till stor grad sammanlänkade genom bland annat betalningar, lån, derivatkontrakt och korsägande. Även på det tekniska planet länkas de samman exempelvis genom att de använder samma hård- och mjukvara samt anlitar samma tjänsteleverantörer för exempelvis IT-drift, telekommunikation eller molntjänster. Det kan öka risken för att cyberattacker sprider sig i det finansiella systemet och kan därmed påverka den finansiella stabiliteten. Aktörer i det finansiella systemet är också i hög grad beroende av data och av samma datakällor, vilket ytterligare ökar sammanlänkningen. Att både finansiella och tekniska tjänster dessutom ofta är gränsöverskridande ökar risken för att konsekvenser av större cyberattacker sprider sig mellan länder.[23]

Den tredje kanalen är den *finansiella kanalen*. Här är fokus på att cyberattacken leder till finansiella förluster för en eller flera aktörer, antingen direkt eller indirekt via förtroendeeffekter eller den operationella kanalen. Finansiella förluster kan i sin tur leda till ytterligare finansiella förluster, försämrat förtroende eller båda.[24]

4. Indirekt påverkan – spridningseffekter leder till ytterligare konsekvenser

De spridningseffekter som vi har beskrivit ovan kan i sin tur påverka samma eller andra aktörer ytterligare, se *indirekt påverkan* i Figur 2. Detta avser alltså effekter som inte var en direkt följd av den initiala attacken och påverkar antingen via spridningskanalerna som beskrivits ovan eller konfidentialitet, riktighet och tillgänglighet precis som vid direkt påverkan. Det kan drabba både organisationer som redan har påverkats direkt och organisationer som dittills varit opåverkade av den initiala attacken. Indirekta effekter kan ses som en följd av spridningseffekterna och kan ta sig uttryck i förlorat förtroende, finansiella förluster samt risken för att en eller flera finansiella

[21] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

[22] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

[23] Se F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden.

[24] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

organisationer hamnar i en negativ spiral av spridningseffekter och ytterligare indirekt påverkan.

5. Påverkan på finansiell stabilitet – risk för att cyberattacken leder till finansiell instabilitet

Som vi har beskrivit ovan finns det flera vägar till påverkan på finansiell stabilitet och detta steg sammanfattar denna påverkan. Vår slutsats av denna analys pekar på att det är fullt möjligt att en cyberattack kan leda till en systemkris i det finansiella systemet. Det stämmer också med tidigare analyser.[25]

Som vi har illustrerat med pilarna i Figur 2 kan cyberattacker påverka den finansiella stabiliteten antingen direkt eller indirekt, eller genom en kombination av båda. Det är möjligt att en cyberattack mot finansiella aktörer eller dess tredjepartsleverantörer påverkar kritiska finansiella funktioner så allvarligt att attacken får en direkt påverkan på den finansiella stabiliteten. Det är även möjligt att den initiala attacken endast gör begränsad skada, men att följdeffekterna sprider sig och förstärks så pass mycket att de slutligen påverkar den finansiella stabiliteten.

De flesta lyckade cyberattacker påverkar enbart en finansiell aktör och orsakar en begränsad skada. Det finns inga kända fall av cyberattacker som har lett till systemkriser.[26] Det betyder dock inte att de inte skulle kunna göra det. En lyckad cyberattack med tillräckliga resurser för att störa en viktig aktör eller sprida effekterna genom det finansiella systemet skulle kunna utgöra en systemrisk.[27] I detta avseende är förtroendekanalen speciellt viktig så att finansiella marknader, företag och allmänheten har förtroende för att det finansiella systemet fungerar.

4 Förståelse för hotbilden är central för att hantera cyberrisk

I tidigare avsnitt har vi beskrivit hur en cyberattack potentiellt kan leda till finansiell instabilitet. Det beror på att aktörer i det finansiella systemet utför funktioner som är kritiska för finansiell stabilitet, och deras verksamheter behöver därmed ha ett väl anpassat skydd för att minimera risken för cyberattacker. För att lyckas med detta behöver skyddet stå i proportion till både verksamhetens skyddsvärden[28] och den hotbild som finns mot verksamheten. Cyberrisk drivs av aktörer med avsikt och förmåga att påverka system eller information i digitala miljöer. En aktör som initierar och står bakom ett cyberhot kallas hotaktör och kan ha olika mål, drivkrafter och metoder.

[25] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden. och F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden.

[26] Se *Systemic Cyber Risk*, februari 2020. Europeiska systemrisknämnden.

[27] Se F. Adelmann, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020) Cyber Risk and Financial Stability: It's a Small World After All, *IMF Staff Discussion Note*. Internationella valutafonden.

[28] Med skyddsvärden avses i detta sammanhang system eller information vars tillgänglighet, riktighet eller konfidentialitet behöver skyddas för att inte oacceptabla konsekvenser ska följa.

Att bedöma hotbilden är med andra ord nödvändigt för att veta vad man behöver skydda sin verksamhet mot.

Att bedöma hotbilden är centralt för att kunna skydda sig

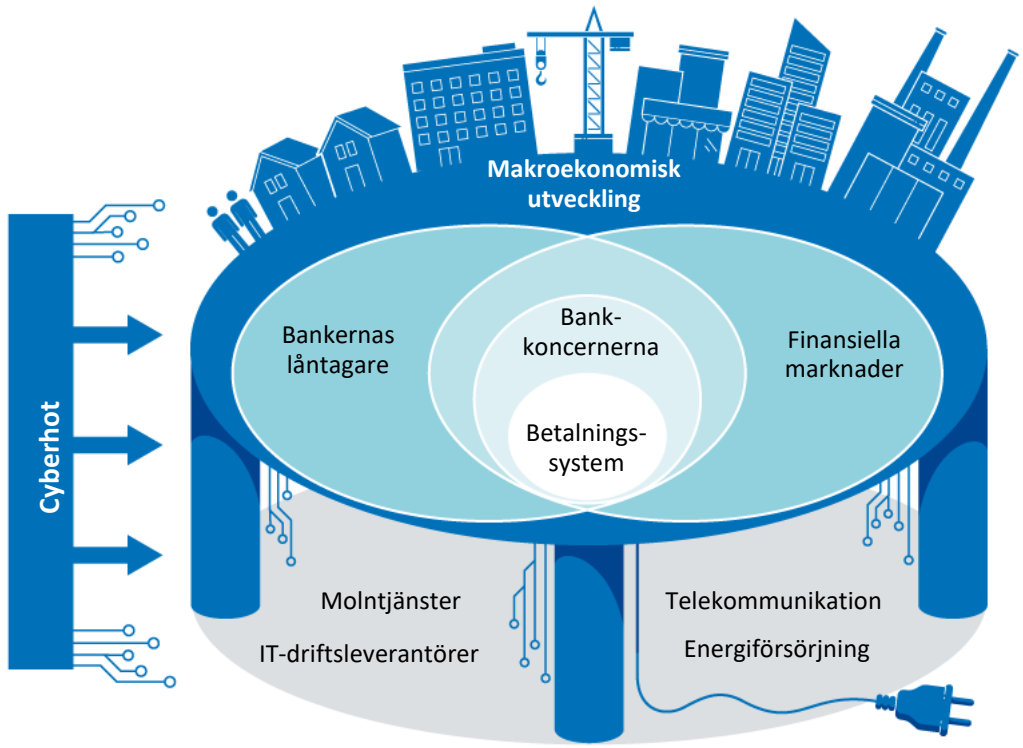
Cyberhot uppstår i det finansiella systemet när en hotaktör har både avsikt och förmåga att utföra skadliga handlingar riktat mot en finansiell verksamhet eller dess tredjepartsleverantörer. Dessa handlingar sker i det som brukar kallas cyberdomänen eller cyberrymden, det vill säga den globala informationsmiljön som består av sammanlänkade IT-infrastrukturer som är beroende av varandra med tillhörande data och information.[29] Men även om en hotaktör har förmåga att göra skada utgör den i regel inget hot så länge den saknar avsikt. På motsvarande sätt utgör inte en hotaktör med avsikt att skada något hot, så länge den saknar förmåga.

Trots att ett hot alltså har relativt lättbegripliga beståndsdelar är det svårt att analysera hotbilden mot en specifik verksamhet. En betydande förklaring till det är att hotbilder ofta varierar över tid och kan förändras snabbt. Vem som har nödvändig förmåga är i allmänhet svårt att bedöma och föränderligt inom cyberdomänen. Metoder för att manipulera, förstöra och otillbörligen tillskansa sig information förändras och skyddsåtgärder går aldrig att förlita sig på helt. De digitala verktyg och sårbarheter som en hotaktör använder sig av är allt annat än konstanta, samtidigt som de IT-miljöer som ska försvaras också ständigt förändras. Hotaktörer tenderar även att återanvända andra hotaktörers verktyg och kan därtill köpa sig viss förmåga.[30] För att fungera korrekt är en modern IT-miljö dessutom ofta beroende av många andra än enbart den egna organisationen. Till detta hör att hotbilden finns mot både det finansiella systemet och dess kritiska leverantörer, vilket illustreras i Figur 4 nedan.

[29] H. Karlzén, H. Granlund och M. Wedlin (2018), Operationer i cyberdomänen - en inventering av svensk forskning, *FOI-R--4594*. Totalförsvarets forskningsinstitut.

[30] H. Karlzén (2020), Cyberoperationer – en slutrapport, *FOI-R--5072*. Totalförsvarets forskningsinstitut.

Figur 4. Cyberhotet riktar sig mot både det finansiella systemet och dess kritiska tjänsteleverantörer



Källa: Sveriges riksbank.

Precis som en hotaktörs metoder och förmåga kan utvecklas och förändras över tid kan också en hotaktörs avsikt förändras. Utrikes- och säkerhetspolitiska förändringar eller medial uppmärksamhet är exempel på händelser som kan påverka en hotaktörs avsikter. Därför är en hotbild kortsiktig och behöver uppdateras löpande.[31]

Bank-, finans- och försäkringssektorns komplexitet försvårar arbetet med att bedöma sektorns hotbild.[32] Europeiska unionens cybersäkerhetsbyrå, ENISA, bedömer dock att cybersäkerhetsrisker i allmänhet kommer att bli ännu svårare att bedöma och tolka under de kommande tio åren på grund av cyberhotets ökande komplexitet och den expanderande attackytan, det vill säga de möjliga ingångarna för angriparen, som följer av den fortsatt snabba digitaliseringen.[33]

Skyddet bör anpassas efter det största hotet

Hotaktörerna har som vi har beskrivit varierande avsikter och förmågor. Som exempel kan organiserad brottslighet initiera cyberangrepp för att nå finansiella mål där ekonomisk vinning är drivkraften, ideologiskt motiverade aktörer kan initiera cyberan-

[31] Se *Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys*, juni 2020. Säkerhetspolisen.

[32] Se *ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis*, oktober 2020. European Union Agency for Cybersecurity.

[33] Se *ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis*, oktober 2020. European Union Agency for Cybersecurity.

grepp för att bedriva aktivism och statliga eller statsunderstödda aktörer kan med politisk drivkraft initiera cyberangrepp med spionage, sabotage eller påverkan som mål. De varierade drivkrafterna, målen och förmågorna innebär att olika hotaktörer kan uppträda mycket olika när det kommer till hur långsiktiga, kvalificerade, målinriktade eller opportunistiska de är i sitt arbete. Detta leder till att olika hotaktörer till viss del kräver olika skydd.

Det största hotet mot den samhällskritiska infrastruktur som det finansiella systemets aktörer gemensamt utgör är statliga och statsunderstödda hotaktörer.[34] Statliga aktörer söker i dag insteg i digital infrastruktur som är kritisk för det svenska samhället för att ha möjlighet att slå ut den i det fall avsikten uppstår.[35] Hotbilden mot Sverige har i dessa sammanhang blivit bredare, mer komplex och bedöms dessutom rikta sig mot politiska, militära och ekonomiska skyddsvärden parallellt.[36] Statliga eller statsunderstödda hotaktörer har med andra ord både avsikt och förmåga att utföra cyberattacker som kan skada centrala samhällsfunktioner i Sverige.[37]

Det är ovan nämnda hot som det svenska finansiella systemet behöver anpassa sina skyddsåtgärder efter. Då hot från statliga aktörer är mer kvalificerade och i regel ställer högre krav på skydd än hot från andra hotaktörer utgör denna typ av hot vad man brukar kalla för det dimensionerande hotet. För hotaktörer med denna typ av kvalificerade förmåga är allt som är kopplat till internet tillgängligt och möjligt att ta sig in i. Till skillnad från många andra cyberhot är dessa attacker dessutom ofta avsedda att inte bli upptäckta.[38] Därmed räcker det inte att försöka stoppa en kvalificerad hotaktör i det initiala skedet. Det finansiella systemets aktörer bör dessutom enskilt och gemensamt och så långt som möjligt ytterligare försvåra sådana angrepp genom att utveckla en förmåga att upptäcka, avfärda och återhämta sig från dem. Att utveckla och upprätthålla sådan förmåga är förhållandevis svårt och kräver tid. Ett viktigt organisatoriskt och kulturellt första steg är att etablera en så kallad ”assume breach”-mentalitet i sin verksamhet, där man utgår från att intrång kommer att ske, redan har skett och kanske till och med äger rum just nu. Åtgärder för att förebygga, hantera och återhämta sig från kvalificerade cyberattacker behöver med andra ord inkludera en hög förmåga att upptäcka när befintliga skyddsåtgärder brustit samt en förmåga att åtgärda såväl brister som de konsekvenser bristerna medför.[39]

En annan viktig del i arbetet med att förbättra motståndskraften ligger i god samordning gällande cyberrisk och en långsiktig planering för minskad sårbarhet för det finansiella systemet. Denna samordning bör involvera både privata och offentliga aktörer inom den finansiella sektorn. Dessutom bör både myndigheter med finansiellt stabilitetsansvar och myndigheter med ansvar för cybersäkerhet delta för att samordningen ska leda till ökad motståndskraft.

[34] Man ska dock komma ihåg att även angrepp som inte nödvändigtvis är särskilt sofistikerade kan göra stor skada, se exempelvis *Internet Organised Crime Threat Assessment (IOCTA)*, oktober 2020. Europol.

[35] Se *MUST Årsöversikt 2020*, mars 2021. Försvarsmakten.

[36] Se *MUST Årsöversikt 2020*, mars 2021. Försvarsmakten.

[37] Se *Säkerhetspolisens årsbok 2019*, mars 2020. Säkerhetspolisen.

[38] Se *FRA årsrapport 2019*, februari 2020. Försvarets radioanstalt.

[39] Se *Finansiell stabilitet*, juni 2016. Sveriges riksbank.

5 Avslutande kommentarer

Slutsatsen av denna analys är att en cyberattack kan påverka den finansiella stabiliteten, och att cyberrisk därmed utgör en systemrisk.

Cyberrisk skiljer sig från andra operativa risker, bland annat genom att cyberattacker kan komma från hotaktörer med ont uppsåt. Cyberrisk karakteriseras också av snabbhet och skalbarhet.

Aktörerna i det finansiella systemet har tydliga incitament att själva hantera den cyberrisk de utsätts för. De utgår dock inte från det övergripande systemperspektivet i sitt arbete, vilket innebär att det finns en risk för negativa externa effekter.[40] Detta innebär en risk för ett marknadsmisslyckande och det finns därmed en naturlig roll för staten att fylla.

För att en organisation ska kunna skydda sig är det avgörande att man förstår både vad som ska skyddas och mot vilka. Åtgärder som syftar till att förebygga och stoppa cyberattacker behöver kompletteras med en förmåga att upptäcka ett bristande skydd samt en förmåga att åtgärda såväl brister som de konsekvenser bristerna medför. Det finns flera sätt att förbättra hanteringen av cyberrisk i det finansiella systemet. Sedan december 2019 koordinerar Riksbanken cybersäkerhetstester enligt TIBER-SE, med syftet att förstärka motståndskraften mot cyberattacker i det svenska finansiella systemet.[41] Vidare är adekvat och fungerande samordning avgörande för att framgångsrikt hantera cyberrisk i det finansiella systemet.

[40] Denna bedömning delas av Finansinspektionen, se *Cyberhot och finansiell stabilitet – FI:s roll och uppgifter*, mars 2021. Finansinspektionen.

[41] Sveriges riksbank, *Riksbanken samordnar cybersäkerhetstester*. Nyhet, senast uppdaterad 13 december 2019. Hämtad 9 maj 2021 https://www.riksbank.se/sv/press-och-publicerat/nyheter-och-pressmeddelanden/nyheter/2019/riksbanken-samordnar-cybersakerhetstester/

Referenser

Adelmann, F., J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz och C. Wilson (2020). "Cyber Risk and Financial Stability: It's a Small World After All", *IMF Staff Discussion Note*. Internationella valutafonden.

Aldasoro, I., L. Gambacorta, P. Giudici och T. Leach (2020). "The drivers of cyber risk", *BIS Working Papers No 865*. Bank for International Settlements.

Bank for International Settlements (2011). "Principles for the Sound Management of Operational Risk", juni.

Bank for International Settlements och International Organization of Securities Commissions (2012). "Principles for Financial Market Infrastructures", april.

European Union Agency for Cybersecurity (2020). "ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis", oktober.

Europeiska systemrisknämnden (2020). "Systemic Cyber Risk", februari.

Europol (2020). "Internet Organised Crime Threat Assessment (IOCTA)", oktober.

Financial Stability Board (2018). "FSB Cyber Lexicon", november.

Finansinspektionen (2021). "Cyberhot och finansiell stabilitet – FI:s roll och uppgifter", mars.

Försvarets radioanstalt (2019). "FRA årsrapport 2018", januari.

Försvarets radioanstalt (2020). "FRA årsrapport 2019", februari.

Försvarets radioanstalt (2021). "FRA årsrapport 2020", mars.

Försvarsmakten (2021). "MUST Årsöversikt 2020", mars.

Gustafsson, T. och D. Lindahl (2019). "Cyberförsvar – färdighet kräver övning", *FOI Memo 6747*. Totalförsvarets forskningsinstitut.

Karlzén, H. (2020). "Cyberoperationer – en slutrapport", *FOI-R--5072*. Totalförsvarets forskningsinstitut.

Karlzén, H., H. Granlund och M. Wedlin (2018). "Operationer i cyberdomänen - en inventering av svensk forskning", *FOI-R--4594*. Totalförsvarets forskningsinstitut.

Sveriges riksbank (2013). "Riksbanken och finansiell stabilitet", februari.

Sveriges riksbank (2016a). "Den svenska finansmarknaden", augusti.

Sveriges riksbank (2016b). "Fördjupning: Cyberhot i det finansiella systemet" *Finansiell stabilitet*, juni.

Sveriges riksbank (2019). ”Riksbanken samordnar cybersäkerhetstester”. Nyhet, senast uppdaterad 13 december 2019. Hämtad 9 maj 2021 https://www.riksbank.se/sv/press-och-publicerat/nyheter-och-pressmeddelanden/nyheter/2019/riksbanken-samordnar-cybersakerhetstester/

Sveriges riksbank (2021). ”Betalningssystemet RIX”, senast uppdaterad 5 mars 2021. Hämtad 8 maj 2021 https://www.riksbank.se/sv/betalningar--kontanter/betalningssystemet-rix/

Säkerhetspolisen (2020a). ”Säkerhetspolisens årsbok 2019”, mars.

Säkerhetspolisen (2020b). ”Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys”, juni.

Säkerhetspolisen (2020c). ”Vägledning i säkerhetsskydd, Informationssäkerhet”, september.

Zouave, E. och M. Jaitner (2019). ”Säkra leverantörskedjor för styrsystem”, *FOI-R—4759*. Totalförsvarets forskningsinstitut.

SVERIGES RIKSBANK
Tel 08 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUKTION SVERIGES RIKSBANK)