

Nationell riskbedömning om finansiering av spridning av massförstörelsevapen

Redovisning av myndighetsgemensamt uppdrag
(Fi2026/00390)

Informationsklass Öppen

Myndighetsgemensam rapport, september 2026

Innehåll

Innehåll	3
1 Inledning	5
1.1 Om regeringsuppdraget.....	5
1.2 Om riskbedömningen.....	5
1.3 Omfattning och avgränsning.....	6
1.4 Övergripande metod och genomförande.....	6
1.5 Regelverk.....	7
2 Den svenska kontexten	9
2.1 Genomförande av internationella sanktioner i Sverige.....	9
2.2 Det ekonomiska sammanhanget	10
2.3 Organiserad brottslighet och kriminell ekonomi	11
2.4 Svensk industri.....	12
2.5 Sveriges arbete för att motverka spridning av massförstörelsevapen	12
2.6 Särskilt om den maritima sektorn	13
2.7 Brott mot internationella sanktioner	13
2.8 Skillnad mellan penningtvätt, terrorfinansiering och finansiering av massförstörelsevapen	15
3 Gränsöverskridande betalningar och värdeöverföringar till Iran 16	16
3.1 Via informella värdeöverföringssystem.....	16
3.2 Via kryptotillgångar	17
3.3 Misstänkta transaktioner till Iran	18
3.4 Förvaltningsärenden kopplade till Iran	19
4 Gränsöverskridande betalningar och värdeöverföringar till Nordkorea.....	20
4.1 Via kryptotillgångar	20
4.2 Misstänkta transaktioner till Nordkorea.....	21
4.3 Förvaltningsärenden kopplade till Nordkorea	21
5 Hot.....	22
5.1 Hot kopplat till internationell handel	22
5.1.1 Sektorer, varor och teknologier med hög risk.....	22
5.1.2 Front- och täckbolag	23
5.1.3 Förtäckt handel	23
5.1.4 Komplexa transaktions- eller anskaffningskedjor, inklusive handel i kryptotillgångar.....	23
5.1.5 Smuggling och illegal handel	23
5.1.6 Illegal finansiell verksamhet (underground banking)	24
5.2 Cyberkriminalitet	24
5.3 Länder och regioner med särskilt hög hotnivå.....	24
5.4 Hot i relation till den svenska kontexten.....	24
6 Sårbarheter	26
6.1 Exponering mot högriskjurisdiktioner	26
6.1.1 Iran.....	26
6.1.2 Gängkriminalitetens koppling till Iran.....	27
6.1.3 Nordkorea	28

6.2	Kunskapsläge och lagstiftning	28
6.3	Tillgång till information.....	29
6.4	Sektorspecifika observationer	30
6.4.1	Särskilt om finansiell sektor	30
6.4.2	Särskilt om icke-finansiell sektor	34
6.4.3	Särskilt om truststrukturer	35
7	Konsekvensbedömning.....	37
7.1	Geopolitiska konsekvenser	37
7.2	Fysiska och miljömässiga konsekvenser	37
7.3	Sociala konsekvenser	38
7.4	Ekonomiska och strukturella konsekvenser.....	38
8	Risker	39
8.1	Oförmåga och underlåtenhet att identifiera tillgångar och företag som ägs eller kontrolleras av sanktionslistade personer ...	39
8.2	Ägande och kontroll döljs genom komplexa företagsstrukturer...	41
8.3	Ägande och kontroll döljs genom transaktionskedjor i flera led ..	42
8.3.1	Avsaknad av motpartsuppgifter	42
8.3.2	Digitala tjänster och gränsöverskridande transaktioner	42
8.3.3	Risker med virtuella bankkonton.....	43
8.3.4	Många mellanhänder och korrespondentbanker, bland annat i tredje land	43
8.3.5	Finansiering via alternativ betalningsinfrastruktur i tredje land	43
8.4	Finansiering genom illegal finansiell verksamhet, så kallad underground banking	44
8.5	Finansiering via kryptotillgångar.....	45
8.6	Finansiering genom försäljning av tjänster och arbetskraft.....	46
8.7	Finansiering genom försäljning av varor	47
9	Samlad bedömning	48

1 Inledning

1.1 Om regeringsuppdraget

Regeringen har givit Ekobrottsmyndigheten, Finansinspektionen, Inspektionen för strategiska produkter, Kommerskollegium, Kustbevakningen, Polismyndigheten, Skatteverket, Säkerhetspolisen, Tullverket och Åklagarmyndigheten i uppdrag att ta fram och offentliggöra en nationell bedömning av riskerna för att riktade ekonomiska sanktioner beslutade av Förenta nationerna om finansiering av spridning av massförstörelsevapen kringgås eller inte genomförs.¹ Uppdraget sker med beaktande av det mellanstatliga organet Arbetsgruppen för finansiella åtgärders (Financial Action Task Force, FATF) rekommendation 1.

Myndigheterna har utsett Polismyndigheten för att hålla samman uppdraget, men samtliga ingående myndigheter står bakom rapporten.

1.2 Om riskbedömningen

Detta är Sveriges nationella riskbedömning av riskerna för att Förenta nationernas (FN:s) riktade ekonomiska sanktioner om spridning av massförstörelsevapen inte genomförs eller kringgås. Bedömningen bygger på en analys av hot, sårbarheter och konsekvenser som kan påverka genomförandet av eller möjligheterna att kringgå de riktade ekonomiska sanktionerna.

Spridning av massförstörelsevapen och de program som stödjer sådan verksamhet utgör ett allvarligt hot mot internationell fred och säkerhet. Riktade ekonomiska sanktioner är ett kraftfullt verktyg för att förhindra att personer, företag och andra aktörer som är involverade i sådan verksamhet får tillgång till egendom och finansiella tjänster.²

Riskbilden är föränderlig och påverkas av såväl geopolitisk utveckling som utvecklingen på betalningsmarknaden, det finansiella systemet, internationella handelsmönster och tekniska innovationer. Trots befintliga kontrollmekanismer och regelverk finns det sårbarheter som kan utnyttjas för att undvika eller kringgå sanktioner.

¹ Regeringsbeslut den 19 februari 2026, Fi2026/00390.

² I EU:s förordningar om restriktiva åtgärder avser riktade ekonomiska sanktioner frysning av ”penningmedel och ekonomiska resurser”. I lagen (2025:327) om internationella sanktioner används istället begreppet ”egendom”.

Arbetet med att genomföra och upprätthålla riktade ekonomiska sanktioner involverar ett stort antal aktörer. Myndigheter med ansvar för tillsyn, kontroll och brottsbekämpning har en central roll, liksom verksamhetsutövare inom den privata sektorn som omfattas av skyldigheter att identifiera och hantera sanktionsrisker.

Syftet med riskbedömningen är att öka förståelsen för de risker som Sverige exponeras för i detta avseende, identifiera områden där sårbarheter kan utnyttjas samt utgöra underlag till förslag på riskreducerande åtgärder. Bedömningen ska även utgöra ett stöd för myndigheter, verksamhetsutövare och andra berörda aktörer i deras arbete med att identifiera, bedöma och hantera risker kopplade till att riktade ekonomiska sanktioner om finansiering av spridning av massförstörelsevapen inte genomförs eller kringgås.

1.3 Omfattning och avgränsning

Riskbedömningens omfattning utgår från FATF:s definitioner av spridning av massförstörelsevapen och finansiering av spridning av massförstörelsevapen, i syfte att identifiera, bedöma och öka förståelsen för risken att sådan spridning sker i enlighet med kraven i FATF:s rekommendation 1.³ Med risken för finansiering av spridning av massförstörelsevapen avses risken för att riktade ekonomiska sanktioner från FN avseende finansiering av spridning av massförstörelsevapen inte genomförs eller kringgås. Bedömningen är därmed avgränsad till de resolutioner som antagits av FN:s säkerhetsråd och som innehåller sådana riktade ekonomiska sanktioner. I dagsläget utgörs dessa av resolutioner som avser antingen Nordkorea eller Iran.

Rapporten är även avgränsad till att identifiera, kartlägga och analysera dessa risker, i enlighet med regeringsuppdraget. Den presenterar därför inga förslag på riskreducerande åtgärder.

EU:s sanktioner mot Ryssland används i denna rapport för att illustrera hur sanktionsregimer generellt hanteras eftersom sanktionerna mot Ryssland utgör det huvudsakliga fokuset för Sveriges sanktionsarbete.

Rapporten omfattar tidsperioden januari 2021 till mars 2026.

1.4 Övergripande metod och genomförande

Rapporten analyserar risker utifrån tre centrala riskfaktorer: hot, sårbarhet och konsekvens.

³ FATF Guidance on Proliferation Financing Risk Assessment and Mitigation, 2021, s. 8.

Hot avser sanktionslistade personer eller entiteter som tidigare har orsakat, eller har förmåga att bryta mot, kringgå eller utnyttja brister i genomförandet av FN:s riktade ekonomiska sanktioner. Hotet kan härröra från tidigare, pågående eller framtida aktiviteter och omfattar även personer eller entiteter som agerar för eller på uppdrag av listade personer eller entiteter. Hot kan vara såväl faktiska som potentiella och varierar i betydelse beroende på land, sektor och verksamhet.

Sårbarhet avser förhållanden som kan utnyttjas av hotaktörer för att möjliggöra finansiering av spridning av massförstörelsevapen. Begreppet omfattar såväl brister i finansiella eller administrativa system som strukturella eller kontextuella faktorer som kan skapa möjligheter för listade personer eller entiteter att samla in, överföra eller på annat sätt disponera medel och andra tillgångar.

Konsekvens avser de effekter som kan uppstå när medel eller andra tillgångar görs tillgängliga för listade personer eller entiteter. Detta kan exempelvis möjliggöra anskaffning av material, komponenter eller tekniska system som krävs för utveckling, produktion eller upprätthållande av illegala kärn-, kemiska eller biologiska vapenprogram samt tillhörande leveranssystem. Eftersom konsekvenserna av finansiering av spridning av massförstörelsevapen är svåra att kvantifiera bedöms de identifierade riskerna i relation till varandra snarare än genom absoluta konsekvensmått.

Arbetet med riskbedömningen har letts gemensamt av Polismyndigheten, Finansinspektionen och Säkerhetspolisen med stöd av samtliga myndigheter som ingår i Sanktionssamverkansrådet. Samtliga myndigheter som givits regeringsuppdraget har utsett Polismyndigheten att hålla samman uppdraget. Analysföretaget Chainalysis har anlåtats för att genomföra en analys av kryptoflöden. Alva Myrdal Center för kärnvapennedrustning har bidragit med sakkunskap och underlag. Data och underlag har även inhämtats från ett urval av finansiella institut samt av Statistiska centralbyrån. Därutöver har samtliga icke-finansiella tillsynsmyndigheter i Samordningsfunktionen mot penningtvätt och finansiering av terrorism givits möjlighet att bidra med synpunkter och underlag.⁴

1.5 Regelverk

Denna riskbedömning är begränsad till de av FN:s säkerhetsråd beslutade riktade ekonomiska sanktionerna – eng. targeted financial sanctions, även kallat ”frysningssanktioner” – mot finansiering av spridning av

⁴ Spelinspektionen, Fastighetsmäklarinspektionen, Revisorsinspektionen samt Länsstyrelserna.

massförstörelsevapen som omfattas av FATF:s rekommendation 7 (Targeted Financial Sanctions Related to Proliferation), vilken hänvisas till i kraven i FATF:s rekommendation 1 (Assessing Risks and Applying a Risk-Based Approach). Rekommendation 7 omfattar alla nuvarande och framtida resolutioner av FN:s säkerhetsråd som innehåller nu aktuell typ av internationella sanktioner. I dagsläget utgörs dessa av resolutioner som avser antingen Nordkorea eller Iran.⁵ Dessa sanktioner implementeras i Sverige genom:

- rådets förordning (EU) 267/2012 om restriktiva åtgärder mot Iran, se särskilt artikel 23 jämte bilaga VIII, samt
- rådets förordning (EU) 2017/1509 om restriktiva åtgärder mot Demokratiska folkrepubliken Korea, se särskilt artikel 34 och bilaga XIII.

Av förordningarna följer att medlemsstaterna är skyldiga att i sin nationella rätt fastställa regler om vilka påföljder som ska tillämpas vid överträdelser av bestämmelser i förordningarna samt att dessa påföljder ska vara effektiva, proportionerliga och avskräckande (se artikel 47 respektive 55). I Sverige genomförs detta genom lagen (2025:327) om internationella sanktioner. Alla typer av överträdelser av förbud, skyldigheter och begränsningar som återfinns i av EU beslutade sanktionsförordningar, liksom överträdelser av villkor i olika tillstånd och liknande beslutade av ansvariga nationella myndigheter, utgör sanktionsbrott enligt samma lag.

⁵ FATF (2021). Guidance on Proliferation Financing Risk Assessment and Mitigation.

2 Den svenska kontexten

2.1 Genomförande av internationella sanktioner i Sverige

Genomförande av internationella sanktioner på nationell nivå sker genom samordning och samverkan mellan ett antal myndigheter med olika ansvarsområden för att säkerställa sanktionsefterlevnad. Övergripande gäller följande:

Utrikesdepartementet (UD) samordnar den svenska sanktionspolitiken. I samverkan med berörda fackdepartement utser UD myndigheter genom regeringsbeslut eller i myndighetsinstruktioner att vara behöriga myndigheter och omhänderta uppgifter som följer av enskilda bestämmelser i EU:s rådsförordningar. UD:s sanktionssamordning bjuder in till samordningsmöten med andra departement och myndigheter med sanktionsansvar⁶. UD har även kontakt med delar av näringslivet som berörs av sanktionerna.

Finansinspektionen (FI) tar emot uppgifter om frysta tillgångar och viss finansiell rapportering. FI prövar även undantag från frysningar i enstaka fall. FI har också i uppdrag att fatta tillfälliga beslut om frysning av tillgångar samt att granska finansiella företags förutsättningar att efterleva EU:s sanktionsförordningar.

Försäkringskassan prövar undantag från frysning av tillgångar för fysiska personer.

Inspektionen för strategiska produkter (ISP) hanterar frågor som rör produkter med dubbla användningsområden, utrustning som kan användas för internt förtryck samt vapenembargon. ISP prövar även tillstånd till frigörande av vissa frysta tillgångar för juridiska personer.

Kommerskollegium hanterar ansökningar om undantag för bland annat export av vissa varor eller tjänster. Kommerskollegium prövar även tillstånd till frigörande av vissa frysta tillgångar avseende juridiska personer. Kommerskollegium tar också emot anmälningar och ansökningar om förhandstillstånd för banköverföringar till Iran.

Polismyndigheten utreder och bekämpar sanktionsbrott. Myndigheten är även behörig myndighet att ta emot uppgifter som underlättar genomförandet av sanktionerna, samt att identifiera och spåra tillgångar. Myndigheten leder även Sanktionssamverkansrådet.

⁶ En fullständig lista över myndigheter som är ansvariga för den svenska sanktionsimplementeringen finns på regeringens hemsida.

Säkerhetspolisen har i uppdrag att förhindra att kunskap, produkter, ämnen eller mikroorganismer förs från eller via Sverige till aktörer som har ambitioner att anskaffa eller vidareutveckla massförstörelsevapen.

Regeringskansliet hanterar tillståndsprövning som avser Sveriges utlandsmyndigheter.

Tullverket kontrollerar att svensk export och import sker i överensstämmelse med sanktionerna.

Sanktionssamverkansrådet (SSR) inrättades som en del av ett regeringsuppdrag i juni 2024. I rådet ingår chefer från Skatteverket, Tullverket, Säkerhetspolisen, Finansinspektionen, Inspektionen för strategiska produkter, Polismyndigheten, Ekobrottsmyndigheten, Kommerskollegium och Åklagarmyndigheten. Sedan januari 2026 är även Kustbevakningen ordinarie medlem. Rådet leds av Polismyndigheten och fattar sina beslut i konsensus. Det finns även två inrättade myndighetsgemensamma expertgrupper under rådet som fokuserar på operativ samverkan och analys. En myndighetsgemensam lägesbild avseende sanktionsefterlevnad i Sverige redovisades till regeringen i januari 2025 och en öppen version publicerades senare under samma år.⁷

SSR:s huvudsakliga inriktning för 2026 är att förstärka arbetet med att implementera de så kallade Rysslandssanktionerna.⁸ Som särskilda fokusområden har SSR pekat ut stödjepunkter till den så kallade Skuggflottan och riktade åtgärder mot prioriterade sektorer inom näringslivet. I övrigt inriktas arbetet mot samverkan och analys, metodutveckling, informationsinsatser, internationell samverkan och återrapporering.

Utöver SSR och UD:s samordningsmöten finns flera nätverk för berörda myndigheter, inklusive ett informellt nationellt myndighetsnätverk och samverkan mellan utbetalande myndigheter för att förhindra ekonomiska transaktioner mellan välfärdssystemen och de entiteter som förekommer på eller har koppling till internationella sanktioner.

2.2 Det ekonomiska sammanhanget

Sverige är en öppen ekonomi med egen valuta, relativt stor finansiell sektor och en hög nivå av digitalisering. Finansmarknaden utvecklas i snabb takt,

⁷ Polismyndigheten (2024). Myndighetsgemensam lägesbild – Efterlevnad av internationella sanktioner.

⁸ I huvudsak EU:s rådsförordning 833/2014 om restriktiva åtgärder mot bakgrund av Rysslands åtgärder som destabiliserar situationen i Ukraina, samt rådsförordning 269/2014 om restriktiva åtgärder med avseende på åtgärder som undergräver eller hotar Ukrainas territoriella integritet, suveränitet och oberoende.

med ständigt nya aktörer och ett växande utbud av tjänster. En tydlig trend är den starka tillväxten hos finansiella företag som bedriver bankliknande verksamhet utan att vara just banker.⁹

Betalningsmarknaden har sett en strukturomvandling och kontanter har i stor utsträckning ersatts med digitala betalsätt, oftast kort eller Swish. I Sverige är Swish den största tjänsten för omedelbara betalningar, en typ av betalsätt som väntas bli allt vanligare.¹⁰

Alla delar av det svenska finansiella systemet är nära sammanlänkade med internationella aktörer och finansmarknader och utlandets betydelse fortsätter att öka. Utlandsbetalningar är en av de största posterna i Riksbankens betalningssystem.¹¹

2.3 Organiserad brottslighet och kriminell ekonomi

Den organiserade brottsligheten i Sverige utgör ett brett och komplext problem med samhällshotande kapacitet. Kriminella nätverk drivs av ekonomisk vinning och är skickliga på att utnyttja samhällets sårbarheter, såväl som den internationella dimensionen, för att främja sin brottsliga verksamhet och maximera sina vinster.¹² Företagssektorn är en viktig gränsyta mellan organiserad brottslighet och den legala ekonomin.¹³

Den kriminella ekonomin i Sverige omsätter stora belopp.¹⁴ Uppskattningar har visat att det kan röra sig om flera hundra miljarder kronor per år.¹⁵ Kontanter bedöms utgöra en stor del av den kriminella ekonomin eftersom det är ett effektivt betalmedel för att undgå bankers och myndigheters kontroller och därmed har en viktig roll i brottsupplägg.

Samhället försöker på olika sätt försvåra och förhindra att pengar från brott omsätts i den legala ekonomin och finansierar ny brottslighet. Lagstiftningen på området har successivt skärpts samtidigt som riskmedvetenheten har ökat

⁹ Riksbanken (2024). Den svenska finansmarknaden.

¹⁰ Riksbanken (2026). Betalningsrapport 2026.

¹¹ Betalningar i svenska kronor som går till eller från en svensk bank som är korrespondentbank för en utländsk bank.

¹² Polismyndigheten (2025). Myndighetsgemensam lägesbild – Organiserad brottslighet 2025.

¹³ SMOB (2026). Samhällsgemensam lägesbild över organiserad brottslighet – Aktörer, relationer och strategiska sårbarheter.

¹⁴ Begreppet kriminell ekonomi definieras som det samlade system av aktiviteter, transaktioner och tjänster där ekonomiska värden skapas, överförs eller döljs genom handlingar som helt eller delvis sker utanför lagliga och reglerade strukturer och processer.

¹⁵ Expertgruppen för studier i offentlig ekonomi (2026). Svarta siffror – en ESO-rapport om den kriminella ekonomins omfattning.

och kontrollsystemen har stärkts. En konsekvens av detta är att brottslig verksamhet förflyttas utanför det legala finansiella systemet.

2.4 Svensk industri

Sverige är en ingenjörsnation med en högteknologisk tillverkningsindustri och en, sett till sin storlek, stor försvarsindustri. Vissa av dessa produkter kan vara av värde i ett massförstörelsevapenprogram. Främst gäller det produkter med dubbla användningsområden (PDA),¹⁶ men även andra produkter kan i vissa fall användas till framställning av massförstörelsevapen.¹⁷

Sverige är ett land med betydande utrikeshandel, export och import, där exportindustrin utgör en viktig del av svensk ekonomi och konkurrenskraft, och med ett flertal stora företag med global räckvidd. Sverige är också en kunskapsnation vars lärosäten och innovationsbolag bedriver forskning i internationell framkant. Vi är beroende av internationellt samarbete och teknikutbyte. Samtidigt kan såväl export av fysiska produkter som överföring av immateriell teknik riskera att bidra till spridning av massförstörelsevapen.

2.5 Sveriges arbete för att motverka spridning av massförstörelsevapen

Intresset hos främmande makt att stjäla, köpa, eller på annat sätt anskaffa svenska produkter, teknik och kunskap är stort.¹⁸ För att motverka risken att svensk export bidrar till spridning av massförstörelsevapen krävs en robust exportkontroll och att exportföretag och forskningsorganisationer har goda processer för kundkännedom, riskbedömning och regelefterlevnad.

Genom exportkontrollen kontrollerar Inspektionen för strategiska produkter (ISP) export av produkter som skulle kunna användas för kemiska, biologiska eller nukleära vapen, eller missiler som kan bära sådana vapen.¹⁹ ISP arbetar aktivt med implementering av exportkontrollregelverket i syfte att förhindra att produkter bidrar till spridning av massförstörelsevapen. Vidare är ISP behörig myndighet för att inom ramen för flera sanktionsregimer

¹⁶ Listade i bilaga I i Europaparlamentets och rådets förordning (EU) 2021/821 (PDA-förordningen).

¹⁷ Av detta skäl innehåller PDA-förordningen en säkerhetsventil i artikel 4, en så kallad *catch-all*-bestämmelse, som möjliggör exportkontroll av produkter om dessa är, eller kan vara, avsedda för massförstörelsevapen.

¹⁸ Säkerhetspolisen (2026). Säkerhetspolisen 2025–2026.

¹⁹ Exportkontrollen grundar sig huvudsakligen i Europaparlamentets och rådets förordning (EU) 2021/821 (PDA-förordningen).

implementera bestämmelser som syftar till att förhindra spridning av massförstörelsevapen.

Sverige deltar aktivt i flera internationella samarbeten som syftar till att motverka spridningen av massförstörelsevapen, bland annat inom de så kallade exportkontrollregimerna. Tre exportkontrollregimer är särskilt inriktade mot att förhindra spridning av massförstörelsevapen och dess bärare: Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR) och Australiengruppen (AG).

2.6 Särskilt om den maritima sektorn

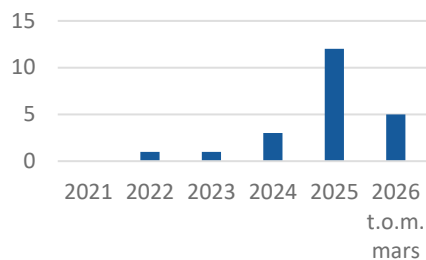
Stora delar av internationell handel sker via sjöfart. Kustbevakningen har i uppdrag att dygnet runt ha en sjölägesbild kopplad till de fartygsrörelser som sker i svenskt vatten och havsområden i anslutning till svensk ekonomisk zon. Kustbevakningen genomför bordning och sjösäkerhetskontroller ombord på fartyg som kan misstänkas ha en falskflaggning eller oklart ägandeskap/registrering. Om Kustbevakningen vid kontroll ombord på fartyg observerar misstänkt last informeras ansvariga myndigheter. Kustbevakningen bedömer att mörkertalet kopplat till felaktig registrering och falsk flaggning är stort.

2.7 Brott mot internationella sanktioner

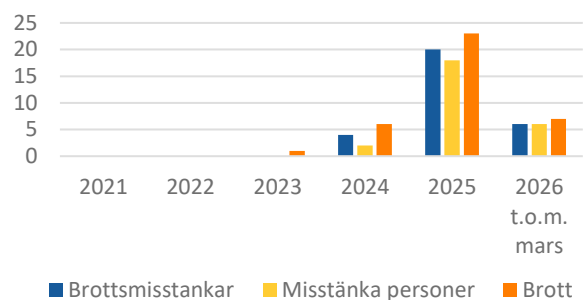
Det finns kriminella aktörer som bryter mot och kringgår de internationella sanktioner som gäller i Sverige, inklusive aktörer knutna till främmande makts underrättelse- och säkerhetstjänster. Antalet anmälda sanktionsbrott till Polismyndigheten är begränsade till ett fåtal, totalt 22 under tidsperioden januari 2021 till och med mars 2026. Likaså är antalet sanktionsärenden som hanterats av Åklagarmyndigheten begränsade, sammanlagt 37 brott, 30 brottsmisstankar, och 26 misstänkta personer.²⁰ I båda fallen syns en tydlig ökning mot slutet av tidsperioden, se figur 1 och 2. Ökningen förklaras främst av EU:s omfattande sanktioner mot Ryssland sedan 2022. Mörkertalet bedöms som stort.²¹ En (1) brottsanmälan kan kopplas till sanktionsregimerna mot Iran och Nordkorea avseende massförstörelsevapen. Det finns dock inga fällande domar med rubriceringen sanktionsbrott under tidsperioden.

²⁰ Eventuella ärenden som hanterats av riksenheten för säkerhetsmål ingår inte i underlaget.

²¹ Polismyndigheten (2024). Myndighetsgemensam lägesbild – Efterlevnad av internationella sanktioner.

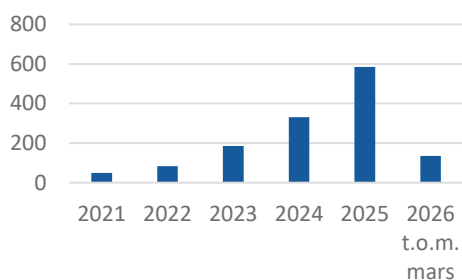
Figur 1 Antal anmälda sanktionsbrott

Källa: Polisen

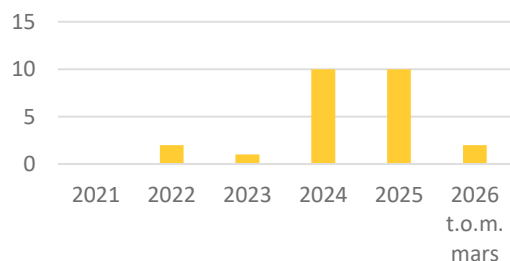
Figur 2 Antal sanktionsärenden hanterade av Åklagarmyndigheten

Källa: Åklagarmyndigheten

Av de misstankerapporter som skickats in under tidsperioden har Finanspolisen identifierat strax under 1 400 rapporter som rör internationella sanktioner och sanktionsbrott, se figur 3,²² samt 25 misstankerapporter som rör massförstörelsevapen, se figur 4.

Figur 3 Antal rapporter till Finanspolisen som rör sanktionsbrott.

Källa: Polisen

Figur 4 Antal rapporter till Finanspolisen som rör massförstörelsevapen.

Källa: Polisen

Sanktionsbrottslighet bedöms ha inslag av samtliga typer av kriminell infrastruktur, vilket avgör dess förmåga att hota skyddsvärda samhällsfunktioner.²³ Aktörerna nyttjar såväl handelsbaserad penningtvätt och brevlådeföretag som kryptotillgångar²⁴ och möjliggörare i den kriminella ekonomin för att dölja de ofta komplexa brottsuppläggen. Pengakurirer,

²² Enligt penningtvättslagen 4 kap 3 § ska verksamhetsutövare rapportera misstänkta aktiviteter och transaktioner till Finanspolisen om de har skäligen grund att misstänka penningtvätt eller finansiering av terrorism eller att egendom härrör från brottslig handling. En misstankerapport är inte samma sak som en brottsanmälan.

²³ Begreppet kriminell infrastruktur omfattar följande kriminella metoder: 1) användande av företag inom brottsområdet, 2) penningtvätt och kriminell ekonomi, 3) oriktiga identiteter och handlingar, 4) korruption eller otillåten påverkan, 5) våld och hot, samt 6) motåtgärder för att undvika upptäckt och lagföring.

²⁴ Se vidare i avsnitt 3.2 om distinktion mellan kryptotillgångar och kryptovalutor.

Hawalaverksamhet och användande av digitala finansiella tjänster i utlandet försvårar ytterligare möjligheterna att upptäcka och förhindra kringgåenden av sanktionerna. Även otillåten påverkan, exempelvis olaga hot, påverkanskampanjer, korruption och i viss utsträckning våld, används för att möjliggöra överträdelser av sanktionsbestämmelser.²⁵

Det är okänt hur stora belopp den illegala indirekta handeln och kringgåendet av sanktioner omfattar. Ny lagstiftning trädde i kraft i juni 2025 vilket förbättrat myndigheternas möjligheter att arbeta mer effektivt på området.²⁶

2.8 Skillnad mellan penningtvätt, terrorfinansiering och finansiering av massförstörelsevapen

Penningtvätt handlar om att kriminella aktörer agerar för att dölja sambandet mellan brottet och brottsvinsten. Det kan röra sig om pengar från narkotikabrott, skattebrott eller bedrägerier som ”tvättas” för att kunna användas i den legala ekonomin. Penningtvätt är ofta en förutsättning för att kriminella ska kunna använda brottsvinsterna.

Finansiering av terrorism handlar om att samla in, tillhandahålla eller ta emot pengar som ska finansiera terrorism. Till skillnad från penningtvätt, som handlar om att dölja tillgångarnas ursprung, handlar finansiering av terrorism om att dölja vad tillgångarna ska användas till. Pengarna kan vara både legalt och illegalt insamlade och förs oftast sedan över till terroristorganisationer i konfliktområden utomlands, men kan även användas för terrorattentat inom landets gränser.²⁷

Finansiering av massförstörelsevapen liknar på vissa sätt både penningtvätt och finansiering av terrorism, penningtvätt i delar som handlar om att dölja medlens ursprung, och finansiering av terrorism i de delar som handlar om insamling av medel för att finansiera brottslig verksamhet utomlands. Det handlar likt terrorfinansiering om att dölja vad tillgångarna ska användas till. Även om syftet med finansieringen skiljer sig åt kan det i många fall vara svårt att avgöra vad finansiella flöden de facto används till, i synnerhet när det gäller aktörer knutna till främmande makt.

²⁵ Polismyndigheten (2025). Myndighetsgemensam lägesbild – Organiserad brottslighet 2025.

²⁶ Lagen (2025:327) om internationella sanktioner.

²⁷ För mer information om Sveriges riskbedömning om penningtvätt och finansiering av terrorism hänvisas till Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2024/2025.

3 Gränsöverskridande betalningar och värdeöverföringar till Iran

Med anledning av de internationella sanktioner som riktats mot Iran under lång tid har möjligheterna att genomföra direkta transaktioner via det reguljära finansiella systemet varit kraftigt begränsade under tidsperioden. Finansiella företag i Sverige, inklusive betaltjänstleverantörer som erbjuder tjänsten penningöverföring (så kallade penningöverförare),²⁸ har i sin årliga rapportering till Finansinspektionen uppgett att de gjort direkta transaktioner om totalt 3745 kr till Iran under 2024 och totalt 0 kr under 2025.

Andra sätt att genomföra gränsöverskridande betalningar är i kryptotillgångar och med kontanter eller andra värdeföremål genom informella värdeöverföringssystem som i bland annat Mellanöstern benämns Hawala.²⁹ Överföringar via Hawala och i kryptotillgångar kan i sig vara legitima, men båda systemen har egenskaper som gör dem attraktiva för illegala syften.

3.1 Via informella värdeöverföringssystem

Hawala är ett tillitsbaserat, informellt sätt att förmedla pengar som är väletablerat inom bland annat den iranska diasporan i Sverige. Systemet bygger på ett nätverk av förmedlare som går i god för tillgångsbelopp för kunders räkning och överföringar sker genom värdeutjämning, dvs. det krävs inget direkt pengaflöde mellan avsändare och mottagare. Beloppen regleras i stället förmedlarna sinsemellan. Ofta sker värdeutjämningen med kontanta medel, vilket ofta är sedlar men kan också vara guld och andra värdeföremål, genom penningkurirer men även överföringar av kryptotillgångar är vanliga.³⁰

Kontantflödet mellan Sverige och andra länder är förenat med anmälnings- och redovisningsskyldighet.³¹ Ett mått på omfattningen av gränsöverskridande transaktioner till Iran är därför kontantdeklarationer till Tullverket. Under tidsperioden januari 2021 till och med mars 2026 har 67 deklarationer till Iran gjorts av 53 individer om totalt knappt 1,6 miljoner

²⁸ Exempelvis Western Union, Moneygram, Paysend, Remitly, Revolut, Wise, WorldRemit och Transfer Galaxy.

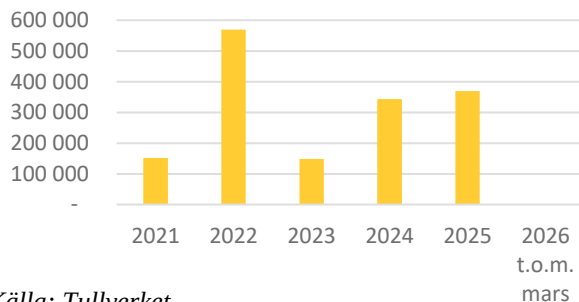
²⁹ Riksbanken (2022). Gränsöverskridande betalningar i fokus.

³⁰ Polismyndigheten (2022). Nationell riskbedömning 2022 – Hawala: värdeöverföringar i alternativa betalningssystem.

³¹ Tullverket arbetar med efterlevnaden av deklarationsplikten för in- och utförsel av kontanta medel överstigande 10 000 EUR. Sedan den 1 april 2026 gäller det även resor till eller från ett annat EU-land. Den som inte fullgör sin deklarationsplikt kan dömas till böter.

euro, se figur 5.³² Av dessa individer förekom var tredje person i polisiära underrättelsesammanhang kopplat till ekonomisk brottslighet. Andelen av dessa överföringar som skett genom Hawala har inte kunnat bedömas. Mörkertalet av kontanter som förs ut från Sverige utan att deklarerats bedöms dock vara stort. Det finns även en påtaglig risk för att systemet missbrukas genom att landet som anges i deklARATIONERNA inte är den egentliga destinationen för kontanterna.

Figur 5 Volym kontantdeklARATIONER till Iran (EUR)



Källa: Tullverket

3.2 Via kryptotillgångar

Det finns flera olika typer av kryptotillgångar, till exempel Bitcoin, som till skillnad från traditionella finansiella tillgångar som aktier och obligationer saknar ett underliggande värde, och stablecoins, vars värde är knutet till andra tillgångar som officiella valutor eller guld. Bitcoin används i stor uträkning av privatpersoner i Iran, medan iranska staten bedöms använda stablecoins på industriell skala för att flytta värden kopplat till handel och anskaffning.³³

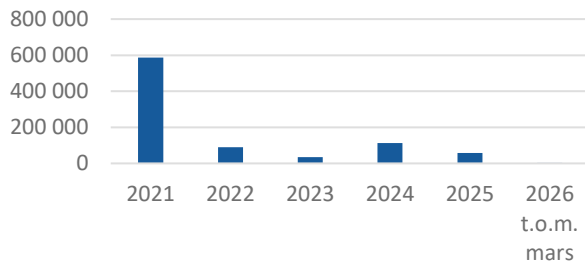
För att få en uppfattning om kryptoflödenas storlek från Sverige till Iran har analysföretaget Chainalysis gjort en kryptoanalys på uppdrag av Polismyndigheten. Den visar bland annat att cirka 277 000 dollar i kryptotillgångar har skickats från svenska leverantörer av kryptotillgångstjänster till Iran mellan januari 2021 och mars 2026; drygt 42 000 dollar direkt och drygt 234 000 dollar indirekt i upp till fem led. Drygt 880 000 dollar har skickats från identifierade illegala svenska tjänster för kryptotillgångar under tidsperioden, se figur 6. Kryptoflödet var som störst under 2021 och har därefter kraftigt minskat. Orsaken till detta är okänd, men det skulle kunna bero på ett ökat användande av mellanhänder, både så kallad

³² För år 2026 fanns för den undersökta perioden till och med mars inga uppgifter om kontantdeklARATIONER till Iran.

³³ Chainalysis (2026). Crypto Crime Report.

no-KYC³⁴ och vanliga kryptobörser, samt verktyg som försvårar spårbarhet och analys.

Figur 6 Volym kryptoöverföringar från Sverige till Iran (USD)



Källa: Polismyndigheten

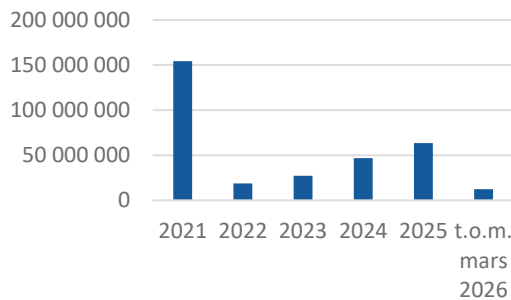
I en bredare analys av svenska kryptoplånböcker utförd av Chainalysis uppskattas cirka 7,7 miljoner dollar i kryptotillgångar ha skickats från Sverige till Iran under tidsperioden, varav cirka 3 miljoner dollar direkt och cirka 4,7 miljoner dollar indirekt. 87 procent av det totala värdet var i Bitcoin, följt av Ethereum och Tron.

Ett sätt att illustrera kryptoflöden till Iran är en fällande dom för grovt penningtvättbrott under 2024. Åtalet avsåg bland annat en person som bedrivit penningförmedling och valutaväxling utan tillstånd, och därigenom mottagit kontanter genom Swish eller banköverföringar för att förmedla värdet i annan valuta till personer i Iran. Inom verksamheten köpte den dömda kryptotillgångar i mycket stor omfattning, och verksamheten omfattade transaktioner till ett värde om minst 82 miljoner kronor under gärningsperioden. (Attunda tingsrätt 2024, målnummer B13832-23.)

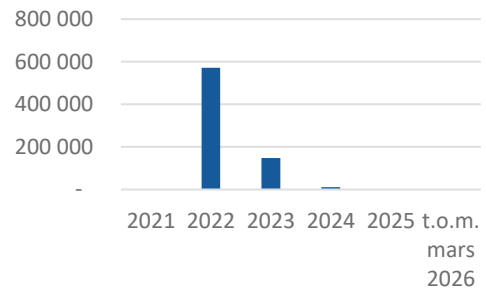
3.3 Misstänkta transaktioner till Iran

Av volymen misstänkta transaktioner som rapporterats under tidsperioden har Finanspolisen identifierat drygt 300 miljoner kronor med koppling till Iran, fördelat enligt figur 7. Ungefär hälften av volymen misstänkta transaktioner rapporterades under 2021. För samma tidsperiod rapporterades totalt drygt 700 000 kronor misstänkta transaktioner i kryptotillgångar, varav merparten under åren 2022–2023, se figur 8.

³⁴ Plattformer med lägre eller obefintliga krav på identifikation av kunden.

Figur 7 Volym misstänkta transaktioner med koppling till Iran (SEK)

Källa: Polismyndigheten

Figur 8 Volym misstänkta transaktioner kryptotillgångar med koppling till Iran (SEK)

Källa: Polismyndigheten

3.4 Förvaltningsärenden kopplade till Iran

ISP har under den aktuella perioden hanterat totalt 802 ärenden avseende export av produkter, överföring av teknik eller tillhandahållande av tekniskt bistånd till Iran. 11 ärenden rörde främst PDA-förordningen³⁵ och 791 ärenden rörde sanktionerna mot Iran. Det är vanligt att ärenden som främst rör PDA-regelverket även berör sanktionsregelverket, eftersom de båda regelverken har samma syfte, dvs. att förhindra spridning av produkter eller teknik till massförstörelsevapenprogram. Att ISP har hanterat ett ärende under perioden innebär att det har inkommit till eller beslutats av myndigheten. Ett ärende kan utmynna i bifall, avslag eller avskrivning.

Kommerskollegium hanterar ansökningar för flera av de undantag som finns i sanktionsregelverken mot Iran. Kommerskollegium har inte tagit emot några ansökningar om undantag från sanktioner för de områden som omfattas av den nationella riskbedömningen men inte heller i övrigt några sanktionsärenden när det gäller Iran under tidsperioden.

Finansinspektionen är behörig myndighet att ta emot information om frysta tillgångar samt bevilja undantag i enstaka fall. I slutet av mars 2026 fanns cirka 170 euro frysta tillgångar tillhörande fysiska personer och knappt 200 000 euro tillhörande juridiska personer, rapporterade under sanktionsregimen mot Iran kopplat till massförstörelsevapen. Dessa fysiska och juridiska personer är dock endast listade av EU och inte av FN. Finansinspektionen har inte hanterat några ärenden kopplat till Iran under tidsperioden.

³⁵ EU:s regelverk för kontroll av produkter med dubbla användningsområden.

4 Gränsöverskridande betalningar och värdeöverföringar till Nordkorea

Nordkorea har befunnit sig under omfattande sanktioner i två decennier och har i praktiken varit avskuret från det globala finansiella systemet under lång tid. Regimen i Nordkorea har till följd av detta utvecklat sofistikerade sätt att kringgå internationella sanktioner och få tillgång till det globala finansiella systemet i syfte att bland annat finansiera sitt massförstörelsevapenprogram, framför allt genom olika typer av storskaliga kriminella upplägg och cyberattacker.³⁶ Nordkorea sänder även medborgare till andra länder för att arbeta och generera intäkter som skickas tillbaka till landet, i synnerhet inom IT-sektorn, men även inom andra branscher.³⁷

Finansiella företag i Sverige har i sin årliga rapportering till Finansinspektionen uppgett att de inte har gjort några direkta transaktioner till Nordkorea. Det finns inte heller några kontantdeklarationer till Nordkorea registrerade hos Tullverket de senaste fem åren. Förekomsten av överföringar via informella värdeöverföringssystem till Nordkorea har inte kunnat bedömas.

4.1 Via kryptotillgångar

När det gäller överföringar via kryptotillgångar har en analys utförd av ett analysföretag på uppdrag av Polismyndigheten visat att cirka 4 200 dollar har skickats från Sverige till Nordkorea under tidsperioden genom indirekta transaktioner i upp till fem led. Inga direkta transaktioner har identifierats. Resultatet innebär dock inte frånvaro av exponering och risk utan är sannolikt en konsekvens av strukturella begränsningar av analysen. Användning av så kallade mixertjänster för kryptotillgångar³⁸ och andra integritetshöjande verktyg bryter blockkedjan och döljer därmed spårbarheten. Analysen visar en betydande exponering mot denna typ av mixertjänster, vilket representerar en potentiell koppling som inte kan identifieras med analysmetoden.

³⁶ Nordkorea bedöms ha spenderat cirka 4 miljarder dollar de senaste 5 åren på sin kärnvapenarsenal. ICAN (2026). Premediated: Nuclear Weapons Spending in 2025.

³⁷ United Nations Security Council (2024). S/2024/215.

³⁸ Till exempel Tornado Cash, Sinbad.io, Blender.io, ChipMixer, ToMix.io.

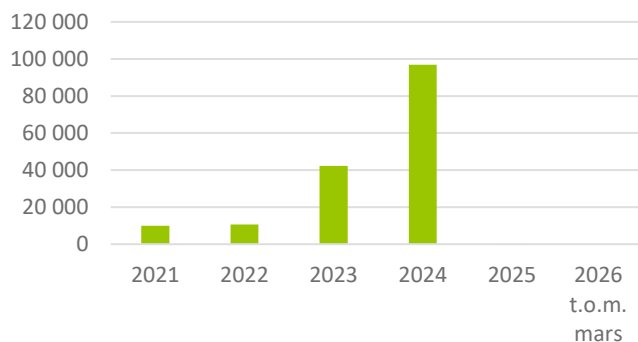
4.2 Misstänkta transaktioner till Nordkorea

Finanspolisen har identifierat två olika sorters misstänkerapporteringar med koppling till Nordkorea. Dessa tillvägagångssätt beskrivs mer utförligt under riskavsnittet.

Den ena varianten rör misstänkta transaktioner som kopplas till storskaliga nordkoreanska kryptostölder. Under 2025 har kryptotransaktioner om totalt 5 600 kronor med koppling till nordkoreanska kryptostölder rapporterats till Finanspolisen.

Den andra varianten rör misstänkta transaktioner som kopplas till nordkoreanska IT-arbetare. Det rör sig om totalt cirka 160 000 dollar över tidsperioden och fördelas enligt figur 9. Transaktionerna har förmedlats av en penningöverförare och rapporterats inom ramen för en större internationell utredning.

Figur 9 Volym misstänkta transaktioner med koppling till Nordkorea (USD)



Källa: Polismyndigheten

4.3 Förvaltningsärenden kopplade till Nordkorea

ISP har inte hanterat något ärende avseende export till Nordkorea.

Kommerskollegium hanterar ansökningar för flera av de undantag som finns i sanktionsregelverken mot Nordkorea. Kommerskollegium har inte tagit emot några ansökningar om undantag från sanktioner för de områden som omfattas av den nationell riskbedömningen men inte heller i övrigt några sanktionsärenden när det gäller Nordkorea under tidsperioden.

Finansinspektionen är behörig myndighet att ta emot information om frysta tillgångar samt bevilja undantag i enstaka fall. I slutet av mars 2026 fanns inga frysta tillgångar rapporterade under sanktionsregimen mot Nordkorea. Finansinspektionen har fattat fyra undantagsbeslut under tidsperioden.

5 Hot

Flera olika stater bedriver verksamhet avsedd att dölja finansiering av massförstörelsevapen. De främsta hoten kommer från de av FN och EU sanktionerade staterna Nordkorea, Iran och Ryssland som genom i huvudsak förtäckta affärsupplägg försöker undvika sanktioner med avsikt att upprätta eller underhålla massförstörelsevapenprogram. Även om Ryssland inte omfattas av FN-sanktionerna bedöms de mekanismer som nyttjas för att kringgå sanktioner användas oberoende av sanktionsregim. Sveriges huvudsakliga arbete mot kringgående av sanktioner riktar sig mot EU:s Rysslandsanktioner. Det är därför relevant att i aktuell analys även se på de mekanismer som används av Ryssland för kringgående av sanktioner.

Utöver de ovan nämnda riskassocierade länderna finns en rad riskfaktorer knutna till internationell handel. Risker att en affärsuppgörelse utgör ett led i finansieringen av massförstörelsevapen ökar om affärspartnern är ett bolag med en kort historik, en otydlig verksamhetsprofil och komplexa och icke-transparenta ägarstrukturer. Flera riskfaktorer är också kopplade till transaktionsmönster, exempelvis att transaktioner sker via ett flertal mellanhänder utan någon tydlig anledning. Andra transaktionsrelaterade riskfaktorer är användandet av korrespondentbanker, användandet av virtuella valutor eller andra förutsättningar som indikerar en önskan om någon typ av ekonomisk dold verksamhet (exempelvis betalningar i kontanter). Sverige utgör ett attraktivt mål med tanke på landets höga teknologiska nivå inom civil och militär industri.

5.1 Hot kopplat till internationell handel

5.1.1 Sektorer, varor och teknologier med hög risk

En stor del av de identifierade riskerna kopplade till finansiering av massförstörelsevapen kan knytas till internationell handel. Särskilt sårbara för finansiering är företag som bedriver verksamhet kopplad till varor eller teknologier som kan användas inom både civil och militär verksamhet, i synnerhet viss typ av avancerad elektronik, industrimaskiner, flygdelar eller kemikalier. En viss risk är också kopplad till handel med antikviteter eller sällsynta metaller eller stenar.

De sanktionerade ländernas finansiering av massförstörelsevapen sker ofta med hjälp av front- eller täckbolag och inte sällan via transaktioner som passerar ett nätverk av mellanhänder. De inblandade frontbolagen sprids medvetet över flera kontinenter för att försvåra upptäckt och motåtgärder från ett enskilt lands myndigheter.

5.1.2 Front- och täckbolag

De sanktionerade ländernas finansiering av massförstörelsevapen sker ofta med hjälp av front- eller täckbolag och inte sällan via transaktioner som passerar ett nätverk av mellanhänder. De inblandade frontbolagen sprids medvetet över flera kontinenter för att försvåra upptäckt och motåtgärder från ett enskilt lands myndigheter.

5.1.3 Förtäckt handel

Aktörer som bedriver affärsverksamhet bör vara uppmärksamma när motpartens beskrivning av avsikten med handeln är generell eller inte överensstämmer med affärspartnerns övriga profil. Likaså bör det betraktas som en varningssignal om företag är ovilliga att lämna information om sin verksamhet.

5.1.4 Komplexa transaktions- eller anskaffningskedjor, inklusive handel i kryptotillgångar

Betalningsinstruktioner som avviker från normalbilden kan också ses som distinkta varningssignaler om att det kan vara ett upplägg för finansiering av massförstörelsevapen. Det kan vara användandet av korrespondentbanker, krav på förbetalning eller användandet av virtuella valutor eller andra förutsättningar som kan kategoriseras som avvikande, och som indikerar en önskan om någon typ av ekonomiskt dold verksamhet och som leder till snabba och icke-transparenta transaktioner. Komplexa transaktionsstrukturer bör också betraktas som en varningssignal, exempelvis när transaktioner sker via ett flertal mellanhänder utan någon tydlig anledning, betalningar som sker via tredje part eller när transaktioner snabbt slussas vidare.

5.1.5 Smuggling och illegal handel

Finansiering av massförstörelsevapen sker också ofta genom en medveten felklassificering av varor eller försök att dölja den faktiska slutmottagaren genom förfalskade slutanvändarintyg. En hög risknivå kan kopplas till länder med svaga penningtvätts- och terrorfinansieringsregleringar och länder som har en icke-transparent företagsmiljö då dessa exempelvis används för att dölja ägarstrukturer. Likaså bör det varningsflaggas för länder med undermålig exportkontroll och tullverksamhet.

5.1.6 Illegal finansiell verksamhet (underground banking)

Finansiering av massförstörelsevapen sker i vissa fall med hjälp av så kallad underground banking för att dölja inkomster genererade från illegal handel. Se vidare beskrivning under riskavsnittet.

5.2 Cyberkriminalitet

En stor risk för finansiering av massförstörelsevapen är också kopplad till cyberkriminalitet exempelvis genom angrepp med utpressningstrojaner i syfte att erhålla ekonomiska medel till den egna staten.

Kryptotillgångar, som beskrivs närmare under avsnitt 6 och 8, kan användas för att kringgå sanktioner och utgör en sårbarhet, till exempel genom stölder av kryptotillgångar. Både Nordkorea och Iran har utvecklat sitt användande av kryptotillgångar för att kringgå finansiella restriktioner. Dessutom har omfattande belopp kommit länderna tillhanda genom cyberkriminalitet, till exempel då kryptotillgångar stulits.

5.3 Länder och regioner med särskilt hög hotnivå

Flera stater bedriver verksamhet avsedd att dölja finansiering av massförstörelsevapen. De främsta hoten kommer dock från de av FN och EU sanktionerade staterna Nordkorea och Iran, samt den från EU sanktionerade staten Ryssland.

5.4 Hot i relation till den svenska kontexten

Myndigheternas bedömning är att metoder för finansiering av massförstörelsevapen blir allt mer sofistikerade och till stor del handlar finansieringen om att kringgå sanktioner. Det är sedan tidigare känt att det sker försök till illegal anskaffning från Sverige av en rad kritiska produkter och spetskompetens med avsikt att föras över till andra länders massförstörelsevapenprogram. Bland de stater som illegalt utvecklar massförstörelsevapenprogram behöver flertalet kunskap från kvalificerad forskning utanför det egna landet och Sverige utgör ett attraktivt mål med tanke på landets höga teknologisk nivå inom civil och militär industri. På Säkerhetspolisens hemsida ges ett exempel på hur ett fall av anskaffning av en produkt med dubbla användningsområden (PDA) från ett svenskt företag kan gå till:

- Ett svenskt företag A, som är tillverkare av en specifik PDA (till exempel vakuumpumpar), kontaktas av företag B med hemvist i ett land utanför EU.

- Företaget B önskar inhandla ett antal pumpar av företag A som söker exporttillstånd vilket godkänns av exportkontrollmyndigheten.
- Företaget B, som produkterna har sålts till, är dock enbart en mellanhand för den egentliga slutmottagaren C.
- Snart sker därför en olaglig vidareexport av produkterna och denna gång till en helt annan slutmottagare (C) än vad det svenska företaget fick information om.
- Slutmottagaren C är istället ett av många företag som ingår i ett massförstörelsevapenprogram och vakuumpumpen från Sverige används till urananrikningsprocess som ett led i målet att tillverka kärnvapen.

6 Sårbarheter

Begreppet sårbarhet i detta sammanhang ska förstås som de faktorer eller situationer som kan utnyttjas, stödja eller underlätta användandet av särskild aktivitet, produkt, service eller andra faktorer för att finansiera spridning av massförstörelsevapen. Sårbarheten kan omfatta specifika sektorer, finansiella produkter eller typer av tjänster vars egenskaper gör dem attraktiva för finansiering av massförstörelsevapen. Sårbarheten kan också inkludera brister i åtgärder som syftar till att förhindra finansiering av spridning av massförstörelsevapen eller särdrag i den svenska kontexten som kan påverka förmågan hos dem som vill finansiera spridning av massförstörelsevapen att skaffa eller flytta medel eller andra tillgångar.

Strukturella sårbarheter avser svagheter i det nationella systemet för att motverka finansiering av spridning av massförstörelsevapen som gör landet attraktivt för sanktionerade personer och entiteter, eller för dem som agerar för deras räkning eller under deras kontroll.

Sektorielementa sårbarheter avser svagheter i – och kontextuella egenskaper hos – en viss sektor som kan leda till att sanktionerade personer och entiteter utnyttjar den för att kringgå sanktioner kopplade till finansiering av spridning av massförstörelsevapen.

6.1 Exponering mot högriskjurisdiktioner

6.1.1 Iran

Sverige har en betydande iransk diaspora, som i huvudsak består av personer som invandrade som flyktingar under 1980-talet samt deras anhöriga som har invandrat senare.³⁹ I april 2026 fanns 625 iranska medborgare registrerade som verkliga huvudmän för svenska företag.⁴⁰ Sveriges handel med Iran är begränsad och har minskat över tid, vilket minskar den övergripande exponeringen men inte nödvändigtvis sårbarheten. Exporten minskade från 229 MSEK år 2020 till 88 MSEK år 2025, med en särskilt tydlig nedgång under senare år från 142 MSEK år 2023 till 89 MSEK år 2024.

³⁹ Byström, Mikael & Frohnert, Pär (2017), *Invandringens historia – från "folkhemmet" till dagens Sverige*, Delmi 2017:5.

⁴⁰ Uppgiften avser registrerat medborgarskap. Bolagsverket registrerar endast ett medborgarskap per person, vilket innebär att personer med dubbelt medborgarskap – exempelvis svenskt och iranskt – kan vara registrerade enbart som svenska medborgare. Antalet personer med iransk bakgrund kan därför vara underskattat.

Samtidigt består exporten alltjämt i stor utsträckning av kemiska produkter och verkstadsprodukter, inklusive organiska kemikalier för diagnostiskt bruk samt olika typer av maskiner och apparater. Dessa varor kan ha användningsområden av strategisk betydelse, vilket innebär att även begränsade handelsvolymen skulle kunna medföra en sårbarhet ur ett icke-spridningsperspektiv.

Sveriges sårbarhet ligger därmed mindre i handelsvolymen som sådan och mer i varusammansättningen, särskilt i de fall komponenter som ventiler, pumpar och precisionsutrustning kan få strategisk betydelse. Detta gäller särskilt mot bakgrund av att kontrollen av slutanvändning kan vara svår, inklusive risk för indirekt vidareexport via tredjeländer.⁴¹

Tullverket har inte haft några ärenden kopplade till sanktioner mot Iran under de senaste åren.

6.1.2 Gängkriminalitetens koppling till Iran

Säkerhetspolisen har konstaterat att den iranska regimen använder kriminella nätverk i Sverige för att utföra våldshandlingar mot andra stater, grupper eller personer i Sverige som uppfattas som ett hot. Deras säkerhetshotande aktiviteter har historiskt framför allt riktat sig mot oppositionella grupper och enskilda individer inom den iranska diasporan. Säkerhetspolisen bedömer att Iran tillsammans med Ryssland och Kina utgör de största säkerhetshoten mot Sverige.⁴²

Gängkriminalitet har under senare år blivit ett växande problem i Sverige. Polismyndighetens bedömning är att det 2025 fanns cirka 17 500 aktiva gängkriminella i Sverige. 81 procent av dem var enbart svenska medborgare, 8 procent var medborgare i både Sverige och ett annat land och 11 procent hade enbart utländskt medborgarskap. Utöver de personer som bedöms som aktiva gängkriminella bedöms cirka 50 000 personer ha kopplingar till aktiva gängkriminella.⁴³

Gängkriminaliteten i Sverige och den särskilda kopplingen till Iran utgör en betydande sårbarhet. Organiserade kriminella nätverk har kapaciteten att möjliggöra illegala internationella flöden av pengar, varor och logistik. Även om gängkriminalitet främst förknippas med narkotikahandel, våldsbrott och utpressning kan det inte uteslutas att motsvarande strukturer utnyttjas för att kringgå sanktioner och exportkontroller.

⁴¹ Kommerskollegiums handelsstatistiska faktablad och SCB.

⁴² Säkerhetspolisen (2024). Iran använder kriminella i Sverige.

⁴³ Polismyndigheten (2025). Lägesbild över aktiva gängkriminella i Sverige.

6.1.3 Nordkorea

Sverige var det första västland som upprättade diplomatiska förbindelser med Nordkorea 1973. Sverige har haft en ambassad i Pyongyang sedan 1975. Den svenska ambassaden fungerar dessutom som så kallad "skyddsmakt" för flera länder som saknar egna diplomatiska relationer eller ambassader i Nordkorea.

I Sverige finns en mycket liten nordkoreansk diaspora, och i april 2026 var ytterst få nordkoreanska medborgare registrerade som verkliga huvudmän för svenska företag. Sveriges handel med Nordkorea är också mycket begränsad. Under perioden 2021–2025 fanns endast mycket små registrerade handelsflöden. Import till Sverige uppgick till 919 000 kronor år 2021 och 9 000 kronor år 2022, medan export från Sverige uppgick till 544 000 kronor år 2022. De få registrerade importposterna avsåg varor såsom kopparstänger och kopparprofiler, vissa vävda tyger samt enstaka klädposter. Den registrerade exporten 2022 avsåg plastskivor och plastfilm. För 2023–2025 fanns ingen registrerad handel.⁴⁴

6.2 Kunskapsläge och lagstiftning

Historiskt har det i Sverige saknats ett uttryckligt krav på att relevanta aktörer, såsom finansiella institut och andra verksamhetsutövare, ska genomföra riskbedömningar avseende bristande efterlevnad eller kringgående av riktade ekonomiska sanktioner. Detta har sannolikt bidragit till att kunskapsnivån inom området inte varit så hög som den annars hade kunnat vara.

Sedan den 30 december 2025 gäller dock Europeiska bankmyndigheten (EBA) riktlinjer om restriktiva åtgärder, vilka innebär att många finansiella institut och vissa andra aktörer ska genomföra verksamhetsanpassade bedömningar av sanktionsrisker, inklusive risker för bristande genomförande och kringgående av sanktioner.⁴⁵

Därutöver kommer det nya EU-regelverket mot penningtvätt och finansiering av terrorism att införa motsvarande krav för en bredare krets av verksamhetsutövare, vilket förväntas bidra till en successivt höjd kunskapsnivå på området.⁴⁶

⁴⁴ SCB (2026).

⁴⁵ EBA (2024). Riktlinjer för interna strategier, förfaranden och kontroller för att säkerställa genomförandet av unionens restriktiva åtgärder och nationella restriktiva åtgärder. EBA/GL/2024/14

⁴⁶ Se artikel 10 (1) Europaparlamentets och rådets förordning (EU) 2024/1624 av den 31 maj 2024 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism (AMLR).

Större svenska banker bedömer generellt att deras direkta exponering mot risker kopplade till finansiering av massförstörelsevapen är begränsad och att den befintliga kontrollmiljön i huvudsak är tillräcklig. Samtidigt kvarstår utmaningar när det gäller att identifiera mer komplexa former av sanktionskringgående, särskilt i fall där riskbilden påverkas av internationella företagsstrukturer och indirekta affärsrelationer.

Det kan i vissa fall innebära att risker kopplade till kundrelationer underskattas, exempelvis när exponering uppstår via dotterbolag, distributörer eller andra affärsförbindelser utanför Sverige.

Sanktionssamverkansrådet som inrättades i juni 2024 förväntas öka kunskapsnivån hos såväl deltagande myndigheter som hos allmänheten genom olika typer av insatser, exempelvis den myndighetsgemensamma lägesbilden om sanktionsefterlevnad som rådet publicerade 2025.

6.3 Tillgång till information

Såväl myndigheter som privata aktörer behöver stärka sin förmåga att förhindra att företag används för att kringgå eller annars utnyttjas i strid med riktade ekonomiska sanktioner. En utmaning i det arbetet har länge varit att offentliga företagsregister inte alltid speglar verkliga förhållanden. Bolagsverket har påbörjat ett utvecklingsarbete i syfte att förbättra registerkvaliteten i sina register men det finns fortfarande brister.

En ytterligare sårbarhet idag är den bristande transparensen avseende aktieägare i onoterade bolag. Detta gör det möjligt för sanktionslistade personer att dölja ägande av fastigheter och andra tillgångar samt försvåra möjligheten att identifiera att företag används för att kringgå sanktioner. För att identifiera ägarförändringar i bolag behöver myndigheter och andra aktörer komplettera Bolagsverkets uppgifter om styrelseförändringar med underrättelseinformation från andra källor.

I Bolagsverkets register över verkliga huvudmän registreras i dagsläget endast ett medborgarskap om det är så att den aktuella personen har flera medborgarskap. Det gör det svårare för myndigheter och verksamhetsutövare att beakta alla risker i kontakter med ett bolag. Detta kommer dock att ändras i samband med införandet av EU:s nya penningtvättsregelverk.⁴⁷

En annan sårbarhet i det svenska systemet är att det är relativt enkelt att starta ett företag, men betydligt mer komplicerat och tidskrävande att avveckla det när verksamheten upphör. Den utdragna avvecklingsprocessen kan leda till att företagare i stället anlitar bolagsbildare och företagsförmedlare som

⁴⁷ Artikel 62(1a) AMLR.

erbjuder snabb avveckling, men där företaget i praktiken säljs vidare som så kallade historikbolag.

Förvärv av historikbolag kräver ingen ny prövning av F-skatt. Genom detta förfarande kan personer och företag som omfattas av sanktioner få tillgång till redan etablerade bolag med kreditvärdighet och nödvändiga registreringar, vilka därefter kan användas för att kringgå riktade ekonomiska sanktioner.

Sårbarheten förstärks ytterligare av att länsstyrelserna, som utövar tillsyn över bolagsbildare och företagsförmedlare enligt penningtvättslagen (PTL),⁴⁸ har konstaterat att många verksamhetsutövare endast genomför kundkännedomsgärder sporadiskt. Flera aktörer uppger dessutom att de inte alltid känner till medlens ursprung. Därtill omfattas dessa verksamhetsutövare inte av någon uttrycklig skyldighet att kontrollera kunder mot relevanta sanktionslistor.

6.4 Sektorspecifika observationer

6.4.1 Särskilt om finansiell sektor

Svenska finansiella institut, framför allt banker, har under närmare två decennier verkat i en miljö där exponering mot Iran och Nordkorea är förenad med mycket höga regelefterlevnadsrisker. Utöver EU-sanktioner har utländska sanktionsregimer, särskilt amerikanska som administreras av Office of Foreign Assets Control (OFAC), ytterligare ökat medvetenheten om sanktionsrisker kopplade till Iran och Nordkorea.

Detta har bidragit till ett genomgående restriktivt förhållningssätt till affärsrelationer och transaktioner med koppling till Iran och Nordkorea. Affärsrelationer, transaktioner och kundengagemang med koppling till dessa länder undviks eller avbryts i stor utsträckning i ett tidigt skede. Sammantaget har utvecklingen bidragit till en hög riskmedvetenhet och en i praktiken låg riskaptit i förhållande till dessa jurisdiktioner.

De största bankernas personal utbildas regelbundet i att hantera sanktionsrisker, men icke-spridningsrisker berörs ofta översiktligt.

Av den periodiska rapportering som samtliga finansiella institut och leverantörer av kryptotillgångar (CASP) ska genomföra enligt penningtvättslagen⁴⁹ kan Finansinspektionen konstatera att dessa saknar

⁴⁸ Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

⁴⁹ 1 kap. 2 § p. 1–13 PTL.

kunder med fast adress i Nordkorea. De fem största bankerna har 152 privatkunder och 10 företagskunder med fast adress i Iran. Bankerna tillämpar olika restriktioner på flera av dessa kunder på grund av sanktionsrisken.

Sanktionsscreening

Den verksamhet som banker bedriver i Sverige omfattar ett stort antal kunder och transaktioner. För att de finansiella instituten ska ha en praktisk möjlighet att efterleva sanktionerna är det ofta nödvändigt att använda ändamålsenliga tekniska verktyg och automatiserade system för sanktionsscreening. Mot den bakgrunden analyserade Finansinspektionen under 2024 i vilken utsträckning bankernas automatiserade system för sanktionsscreening upptäckte sanktionerade personer och företag samt transaktioner kopplade till sådana aktörer. Av kartläggningen framgick att ingen bank uppnådde fullgod träffsäkerhet i den automatiserade kontrollen.

Trots att inget system fullt ut kunde upptäcka alla sanktionerade namn i testmiljö, bedömde FI att bankerna över lag hade en god förståelse för sanktionsreglerna och hade de tekniska lösningar som krävdes för att kunna följa lagkraven. Vidare visade analysen att träffsäkerheten i bankernas sanktionsscreening tenderade att öka ju större banken var. En konsekvens av detta skulle kunna vara att riskerna koncentreras till små och medelstora banker.

Kundkännedom

En ytterligare sårbarhet är kopplad till kvaliteten i kundkännedomsarbetet (Know Your Customer, KYC). Om uppgifter om kunder inte är uppdaterade och tillräckligt tillförlitliga försvåras möjligheten att genomföra träffsäker sanktionsscreening. Detta har särskild betydelse i förhållande till högriskjurisdiktioner som Iran och Nordkorea, där statliga och statsnära aktörer ofta verkar genom komplexa och indirekta strukturer. Brister i identifieringen av exempelvis verkliga huvudmän eller personer i ledande ställning, såsom styrelseledamöter, kan medföra att kopplingar till sanktionerade personer eller nätverk inte upptäcks. Därmed ökar risken för att svenska aktörer, utan vetskap om det, exponeras mot transaktioner som har koppling till sanktionskringgående eller finansiering av massförstörelsevapen.

Omedelbara betalningar

Omedelbara betalningar innebär att medel överförs med mycket kort genomförandetid. De korta tidsramarna ställer höga krav på att sanktionsscreening och andra kontrollåtgärder fungerar effektivt. För de betalningar som omfattas av EU:s regelverk för omedelbara betalningar baseras sanktionskontrollen i större utsträckning på löpande screening av kunder än på granskning av enskilda transaktioner före genomförandet.

En central utmaning är att säkerställa att screening och hantering av potentiella träffar fungerar kontinuerligt, även utanför ordinarie arbetstid. Detta ställer krav på bemanning, automatisering och snabba beslutsprocesser. Brister i dessa förmågor kan öka risken för att sanktionerade personer eller transaktioner inte identifieras i tid.

Mot denna bakgrund ökar omedelbara betalningar betydelsen av effektiva processer för sanktionsscreening och andra riskbegränsande kontroller. Om sådana kontroller inte är tillräckligt effektiva finns en risk att sanktionerade personer eller transaktioner inte identifieras, eller identifieras efter att överföringen redan skett.

Kryptotillgångar

Kryptotillgångar används i ökande utsträckning som ett verktyg för att kringgå finansiella restriktioner och upprätthålla tillgång till internationella marknader. Under 2025 ökade värdet av sanktionsrelaterade kryptotransaktioner markant, och en betydande del av den identifierade aktiviteten kan kopplas till statliga eller statsanknutna aktörer.

När det gäller Iran pekar flera analyser på att kryptotillgångar etablerats som en kompletterande finansiell kanal för staten och dess närstående strukturer, inklusive Islamiska revolutionsgardet (IRGC). Bedömningar från internationella analysföretag indikerar att iranska aktörer genomförde kryptotransaktioner motsvarande mer än 10 miljarder dollar under 2025. En del av dessa flöden bedöms ha koppling till statligt kontrollerade eller statsnära nätverk. Undersökande rapportering visar dessutom att betydande kryptoflöden i vissa fall kan kopplas till finansiering av militära strukturer och proxynätverk.

Kryptotillgångar används också för att möjliggöra finansiering av aktiviteter med koppling till utveckling av militära förmågor, inklusive anskaffning av produkter med dubbla användningsområden. Analyser pekar på att Irananknutna nätverk använder kryptotillgångar för att stödja regionala aktörer, genomföra handel med sanktionerade varor samt finansiera inköp av utrustning som kan användas både civilt och militärt.

Även i relation till Nordkorea framträder tydliga sårbarheter ur ett icke-spridningsperspektiv. Nordkoreanska aktörer har utvecklat en systematisk användning av kryptotillgångar som intäktskälla, främst genom omfattande cyberangrepp mot kryptobörser och andra aktörer i ekosystemet. Under 2025 uppskattas nordkoreanska aktörer ha tillgodogjort sig över 2 miljarder USD genom sådana angrepp. Dessa medel omsätts därefter via komplexa transaktionskedjor, inklusive användning av så kallade mixer-tjänster och blockkedjebryggor, i syfte att dölja ursprung och möjliggöra vidare användning. Intäkterna bedöms i flera analyser utgöra en viktig finansieringskälla för landets kärnvapen- och missilprogram.

Samtidigt framträder tydliga sårbarheter kopplade till hur dessa transaktioner genomförs. Statligt stödda nätverk kombinerar ofta kryptotransaktioner med mer traditionella upplägg för sanktionsundandragande. Det kan handla om användning av mellanhänder, parallella kontostrukturer och komplexa internationella transaktionskedjor som försvårar identifiering av verklig huvudman och transaktionernas syfte. I uppmärksammade fall har betydande transaktioner kunnat genomföras trots att varningssignaler identifierats inom finansiella system, vilket tyder på brister i nuvarande kontrollmekanismer.⁵⁰

Ur ett svenskt perspektiv innebär denna utveckling flera typer av sårbarheter. Sverige har en relativt välutvecklad digital ekonomi och en aktiv användning av kryptotillgångar bland både privatpersoner och företag. Svenska aktörer verkar som förmedlare, handelsplattformar och leverantörer av tekniska infrastrukturtjänster, vilket innebär att internationella kryptoflöden – även sådana med koppling till sanktionsundandragande eller statligt driven finansiering – i praktiken kan beröra eller passera genom svenska aktörer.

En central sårbarhet är därmed risken att svenska aktörer, medvetet eller omedvetet, används som mellanled i internationella transaktionskedjor. De komplexa strukturer som beskrivits ovan försvårar möjligheterna att identifiera motparter och transaktioners faktiska syfte, vilket ökar risken för exponering mot sanktionerade aktörer eller nätverk kopplade till finansiering av massförstörelsevapen.

Vidare innebär den nordkoreanska användningen av cyberangrepp att även svenska aktörer inom kryptosektorn kan utgöra potentiella mål. Angreppen är i grunden globala och opportunistiska, vilket innebär att även aktörer i mindre marknader kan utnyttjas som ingångspunkter. Detta kan leda till att medel med ursprung i angrepp mot svenska eller EU-baserade system indirekt används i finansiering av massförstörelsevapen.

En ytterligare sårbarhet rör så kallad sekundär exponering. Svenska aktörer kan ingå i transaktionsflöden där tillgångar tidigare har passerat genom nätverk kopplade till exempelvis Iran eller Nordkorea, utan att detta är direkt synligt. Detta gäller särskilt vid användning av stablecoins och andra lätt överförbara kryptotillgångar, där värden kan flyttas snabbt mellan olika plattformar och jurisdiktioner.

Samtidigt finns faktorer som bidrar till att begränsa riskerna. Kryptotjänster i Sverige omfattas av regelverk avseende penningtvätt, finansiering av terrorism och sanktionsgenomförande. På EU-nivå innebär införandet av

⁵⁰ Chainalysis (2026). Crypto crime report.

MiCA-förordningen⁵¹ och relaterade tillsynskrav en stärkt ram för tillstånd, kundkännedom och transaktionsövervakning. Dessa åtgärder bedöms ha en dämpande effekt på riskerna.

Regleringen innebär dock inte att sårbarheterna elimineras. Kryptotillgångars gränsöverskridande och delvis decentraliserade natur gör det möjligt att kringgå nationella och europeiska kontrollmekanismer. Sammantaget kvarstår därmed en sårbarhet för att kryptotillgångar indirekt används i flöden som stödjer finansiering av massförstörelsevapen, även i en svensk kontext.⁵²

6.4.2 Särskilt om icke-finansiell sektor

Varuhandeln är en lättillgänglig sektor med möjlighet att handla med kontanter. Detta innebär att transaktioner kan ske väldigt snabbt samtidigt som anonymiteten kan vara hög eftersom kontanter minskar spårbarheten. Lyxartiklar såsom smycken och bilar kan också agera som värdebärare genom att sådana varor förs ut ur Sverige för att vidareförmedlas till sanktionslistade personer.

Varuhandlare ska vidta kundkännedomsåtgärder, när affärsförbindelser etableras med kunder där transaktioner med kontanter uppgår till motsvarande 5 000 euro eller mer.⁵³ Därtill måste åtgärder alltid vidtas när det finns misstankar om penningtvätt eller finansiering av terrorism, oavsett transaktionens storlek eller om den genomförs med kontanter eller på annat sätt.⁵⁴ Till skillnad från vad som gäller i den finansiella sektorn finns i dagsläget ingen särskild skyldighet för varuhandlare att göra kontroller mot sanktionslistor.

Medvetenheten om risker liksom kunskap om riktade ekonomiska sanktioner bedöms vara låg i sektorn. Allvarliga brister i regelefterlevnad gällande bland annat regler om kundkännedom har uppmärksamrats vid länsstyrelsernas tillsyn av sektorn. Därtill sker köp och transaktioner i de flesta fall genom ett

⁵¹ Europaparlaments och rådets förordning (EU) 2023/1114 av den 31 maj 2023 om marknader för kryptotillgångar och om ändring av förordningarna (EU) nr 1093/2010 och (EU) nr 1095/2010 samt direktiven 2013/36/EU och (EU) 2019/1937.

⁵² Chainalysis, *Crypto Sanctions: 2026 Crypto Crime Report* och relaterade analyser (bland annat om statliga aktörers ökade användning av kryptotillgångar, Nordkoreas intäkter från cyberangrepp och kopplingar till massförstörelsevapenprogram); Wall Street Journal, 2026-05-24 (uppgifter om omfattningen av iranska kryptoflöden och kopplingar till IRGC, inklusive TRM Labs uppskattningar av iranska kryptotransaktioner överstigande 10 miljarder USD under 2025).

⁵³ 1 kap. 2 § p. 16 och 3 kap. 6 § PTL.

⁵⁴ 4 kap. 2 § PTL.

fysiskt möte med kunden, vilket betyder att hotfulla situationer kan uppstå som gör det svårare att neka köpet.

Kontanter och värdeföremål utgör en möjlig kanal för värdeöverföring utanför det reguljära finansiella systemet. Sådana tillgångar kan användas för att kringgå finansiell tillsyn och sanktionskontroller, särskilt för aktörer med begränsad tillgång till banksystemet, exempelvis vid kopplingar till Iran eller Nordkorea.

Kontanter kännetecknas av låg spårbarhet och kan användas i upplägg där aktörer vill minska insyn i finansiella flöden. De kan även fungera som ett komplement till andra metoder, såsom handelstransaktioner eller digitala värdeöverföringar.

Sammantaget innebär detta att risker kopplade till icke-spridningsfinansiering inte enbart är begränsade till det formella finansiella systemet, utan även omfattar fysiska värdeöverföringar som i vissa fall kan kopplas till internationella nätverk.

6.4.3 Särskilt om truststrukturer

En trust innebär att någon förvaltar en egendom för någon annans räkning. Det handlar om en juridisk konstruktion där stiftarens äganderätt överförs till en förvaltare på ett visst bestämt sätt.

Truster saknar rättskapacitet, det vill säga förmåga att bära rättigheter och skyldigheter, och är en företeelse som huvudsakligen förekommer i anglosaxiska rättssystem. Av legala skäl finns trusters inte i svensk rätt, men kan förvaltas i Sverige⁵⁵ och därför stå under länsstyrelsernas tillsyn enligt PTL.⁵⁶ Själva trusten finns dock alltid utomlands. Det svenska regelverket är tillämpligt på gränsöverskridande verksamhet som bedrivs av svenska företag eller av utländska företagsetableringar i Sverige.

Trustförvaltningstjänster kan erbjudas yrkesmässigt av både fysiska och juridiska personer, men bedrivs oftast i form av kommanditbolag. Trustförvaltaren ansvarar för förvaltningen av trustens tillgångar, vilka ofta är placerade genom offshorekonton. Tillgångarna kan bestå av exempelvis kontanta medel, värdepapper, fastigheter och kryptovalutor.

Den struktur som en trust erbjuder kan möjliggöra en hög grad av anonymitet för de personer som står bakom verksamheten. Detta innebär en risk för att trusters används för att kringgå eller överträda riktade ekonomiska sanktioner.

⁵⁵ Prop. 2016/17:173 Ytterligare åtgärder mot penningtvätt och finansiering av terrorism, s. 459.

⁵⁶ 1 kap. 2 § p. 22 och 4 § 1 stycket PTL.

Länsstyrelserna, som utövar tillsyn över trustförvaltare, har inom ramen för vandelsprövningar av företrädare för trustförvaltare ofta svårigheter att komma i kontakt med dessa, eftersom de inte sällan är bosatta utomlands.

Den begränsade insynen i sektorn, i kombination med den anonymitet som strukturerna kan erbjuda, gör området särskilt sårbart för överträdelser av eller kringgående av riktade finansiella sanktioner.

7 Konsekvensbedömning

Konsekvenser av att riktade ekonomiska sanktioner om finansiering av spridning av massförstörelsevapen inte genomförs eller kringgås avser följden av att tillgångar görs tillgängliga för listade personer och entiteter. Detta kan möjliggöra anskaffning, utveckling och underhåll av illegala kärnvapen, biologiska eller kemiska vapen samt vapenbärare som ballistiska robotar och kryssningsrobotar. Konsekvenserna från hotet om användning eller användning av massförstörelsevapen avser därmed de effekter och skador som kan uppstå.

7.1 Geopolitiska konsekvenser

När regimer som Iran och Nordkorea får tillgång till finansiering som kan användas till illegal anskaffning och utveckling av massförstörelsevapen ökar hotet om dess användning. Det nuvarande omvärldsläget präglas av geopolitisk turbulens, inte minst den geopolitiska situationen i och omkring Iran. Begränsningar av Irans kärntekniska program kan vägas bland annat mot sanktionslättnader. Regimen i Nordkorea prioriterar sitt kärnvapenprogram och en stärkt finansiering kan skynda på dess utveckling.

Kärnvapenhotet är existentiellt för mänskligheten och har direkta konsekvenser för politiska relationer. Den nuvarande globala hanteringen av kärnvapenhotet, genom ickespridningsregimen, bygger på att antalet kärnvapenarsenaler är begränsat till ett fåtal stater, där varje ytterligare kärnvapenbeväpnad stat innebär en tydligt ökad utmaning med att nå målsättningarna för regimen. Denna ordning befinner sig redan i ett läge av 'strukturell stress', genom den betydande svårigheten i att hantera kärnvapeninnehav hos stater. Det finns en betydande risk att 'det nukleära tabut' bryts genom att tröskeln för staters användning sänks, till exempel genom att så kallade 'taktiska' kärnvapen framstår som legitima för att bekämpa antagonister.

7.2 Fysiska och miljömässiga konsekvenser

De fysiska och miljömässiga effekterna av användningen av kärnvapen är enorma och långtgående. Utöver direkta effekter och skador av en kärnvapenexplosion får det långsiktiga effekter på människa och miljö som kan påverka det globala klimatet. Även ett regionalt begränsat kärnvapenkrig

skulle kunna leda till en så kallad atomvinter, vilket är en hypotetisk köldperiod som i sin tur skulle kunna orsaka massvält.⁵⁷

7.3 Sociala konsekvenser

Användning av kärnvapen orsakar katastrofala effekter där till exempel statsapparaten hela funktion och existens kan undermineras. De humanitära konsekvenserna även bortom direkta dödsoffer är enorma. Det skulle få bestående sociala, psykologiska och fysiska konsekvenser i generationer, genom posttraumatisk stress, strålningsskador och cancer.

7.4 Ekonomiska och strukturella konsekvenser

Förutom att de omfattande och allvarliga direkta skadorna skulle få stora ekonomiska konsekvenser för samhället och enskilda, skulle vetskapen om att aktörer i den offentliga eller privata sfären har använts eller utnyttjats för att finansiera användning massförstörelsevapen förmodligen orsaka anseendeskador både för det finansiella systemet och för staten. Det skulle sannolikt också innebära straffåtgärder från myndigheter och/eller det internationella samfundet.

Utöver detta finns även andra typer av ekonomiska konsekvenser för enskilda. Samtidigt som arbetet mot finansiering av massförstörelsevapen stärker det finansiella systemets integritet, medför det en risk för så kallad derisking, där finansiella institut av försiktighetsskäl avslutar eller begränsar kundrelationer i högriskmiljöer även när riskerna är hanterbara. Konsekvensen kan bli att legitima finansiella flöden stryps vilket kan innebära svårigheter för personer med koppling till exempelvis Iran att tillgodogöra sig grundläggande finansiella tjänster.

⁵⁷ Svenska läkare mot kärnvapen (2026). Den sista vintern: om mänsklighetens överlevnad efter ett kärnvapenkrig; FOI (2021). Kärnvapenscenario för räddningstjänst.

8 Risker

I följande avsnitt beskrivs de risker för att riktade ekonomiska sanktioner från FN om finansiering av spridning av massförstörelsevapen inte genomförs eller kringgås som har identifierats inom ramen för denna nationella riskbedömning. Generella risker och sårbarheter som kopplas till olika sektorer på systemnivå beskrivs mer utförligt i den nationella riskbedömningen av penningtvätt och finansiering av terrorism i Sverige 2024/2025.

8.1 Oförmåga och underlåtenhet att identifiera tillgångar och företag som ägs eller kontrolleras av sanktionslistade personer

En övergripande risk som gäller för samhällets olika sektorer är oförmåga och underlåtenhet att identifiera tillgångar och företag som ägs eller kontrolleras av sanktionslistade personer. Denna risk avser i stor utsträckning finansiella företag som hanterar betalningar och kunders tillgång till finansiella tjänster samt exporterande företag som säljer varor och tjänster, men även myndigheter som gör utbetalningar och upphandlar tjänster.

Många företag använder kommersiella tjänster för sanktionsscreening för att kunna hantera denna risk. Träffsäkerheten i dessa system varierar och vid analys⁵⁸ av bankers tekniska lösningar gjordes bedömningen att det fanns en förhöjd risk hos små och medelstora banker jämfört med större banker. Även variationer i stavning av namn och andra uppgifter kan medföra att sanktionerade parter inte identifieras av bankernas system. I takt med att omedelbara betalningar blir allt vanligare är bedömningen att denna risk kommer att öka, eftersom sanktionskontrollen i mindre utsträckning baseras på granskning av enskilda transaktioner och i större utsträckning på löpande screening av kunder.⁵⁹ Samtidigt utvecklas lösningar för att möjliggöra snabbare gränsöverskridande betalningar, även mellan olika valutor och betalningssystem. Detta kan innebära att tillgångar förflyttas snabbare än tidigare, vilket ökar betydelsen av effektiva processer för sanktionsscreening och andra riskbegränsande kontroller.

Företag som bedriver exportverksamhet behöver göra noggranna kundkontroller för att säkerställa att det inte finns bakomliggande kopplingar till sanktionerade entiteter, även i förhållande till företag som ägs eller

⁵⁸ Finansinspektionen (2024). Fördjupad analys om bankers system för sanktionsscreening.

⁵⁹ I enlighet med artikel 5d i rådsförordning 2024/886 vad gäller omedelbara betalningar i euro. För medlemsländer som inte har euro som valuta börjar kravet gälla under 2027.

kontrolleras av en listad entitet. Att genomföra de fullständiga och heltäckande kundkontroller som krävs kan dock vara svårt – särskilt för små och medelstora företag med begränsade resurser. Svårigheter består bland annat i att förstå att ett ägarskap av en listad entitet innebär ett handelsförbud med ett företag längre ner i företagsstrukturen, att identifiera ägare eller andra personer som utövar kontroll över ett företag, samt att göra genomgående kontroller av samtliga bolag inom en koncern. Samtidigt kan de ekonomiska incitamenten att genomföra affärerna vara höga. Sammantaget innebär dessa utmaningar en risk för att tillgångar indirekt och omedvetet görs tillgängliga för sanktionerade entiteter.

Gällande EU:s sanktioner mot Ryssland finns ett uttryckligt krav för exporterande företag att vidta lämpliga åtgärder, inklusive riskbedömningar, för att hantera risker.⁶⁰ Motsvarande krav återfinns dock inte i sanktionsregimerna kopplade till massförstörelsevapen. Det råder även rättslig oklarhet kring tillämpning av EU:s dataskyddsförordning i relation till internationella sanktioner och i vilken utsträckning företag som inte är särskilt undantagna, vilket bland annat innefattar flera av Sveriges största exportföretag, behöver ansöka om tillstånd från Integritetsskyddsmyndigheten för att kunna använda screeningtjänster för att följa kraven på kundkännedom.⁶¹

Myndigheter har som regel endast direkt översyn och kontroll över tillgångar i form av penningmedel/utbetalningar som en sanktionerad individ innehar hos myndigheten, exempelvis saldot på skattekontot. För att identifiera andra typer av tillgångar behöver normalt sett en utredning inledas. Vissa myndigheter har direkt tillgång till uppgifter om andra typer av tillgångar och bolagsengagemang genom sina verksamhetssystem, exempelvis inkomstuppgifter eller fordons- och fastighetsinnehav. Myndigheter kan begära ut och dela uppgifter om sanktionerade personers tillgångar och penningmedel/utbetalningar med andra myndigheter under vissa förutsättningar. Det saknas emellertid bestämmelser och praxis kring hur andra typer av lös och fast egendom än penningmedel på konton, exempelvis

⁶⁰ Artikel 12gb i rådets förordning (EU) 833/2014 om restriktiva åtgärder mot bakgrund av Rysslands åtgärder som destabiliserar situationen i Ukraina.

⁶¹ Den rättsliga oklarheten gäller om uppgifter om riktade ekonomiska sanktioner omfattas av lydelsen i artikel 10 i dataskyddsförordningen. En person kan vara föremål för en riktad ekonomisk sanktion utan att personen i sig är misstänkt för eller har begått ett brott eller är föremål för en säkerhetsåtgärd som hänger samman med något av detta. (Fi2026/01654 EU:s penningtvättspaket). I praktiken gäller oklarheten de företag som inte står under tillsyn av Finansinspektionen, Inspektionen för strategiska produkter och Strålskyddsmyndigheten. Se IMYFS 2024:1.

fordon, kontanta medel eller fastigheter, ska identifieras och frysas och vilken myndighet som är behörig att genomföra sådana åtgärder.

Det finns också en risk för fördröjt genomförande av FN:s sanktioner och att en sådan tidsfördröjning möjliggör att sanktionslistade entiteter kan tillgodogöra sig tillgångar.⁶² Ett sätt att hantera denna risk är att Finansinspektionen sedan 2024 fattar interimistiska beslut om frysning av tillgångar som gäller innan EU har genomfört sanktionerna.

8.2 Ägande och kontroll döljs genom komplexa företagsstrukturer

Företag och företagskonton kan vara ett effektivt sätt att dölja syftet med överföring av medel. Erfarenheter från arbetet mot penningtvätt visar att aktörer använder företag och företagskonton systematiskt för att kunna överföra stora belopp i kriminella syften. Transaktioner i företag kan passera obemärkt förbi i bankernas kontrollsystem genom exempelvis vinstutdelning, koncerninterna överföringar eller upplägg med osanna fakturor. Företagen kan dessutom ha bankkonton i olika banker och i olika länder, vilket gör det möjligt att slussa stora belopp i flera steg för att försvåra upptäckt och på så sätt kringgå sanktioner.

Det faktum att enskilda banker ofta har en fragmenterad bild av konton och transaktioner i företag gör det svårare att upptäcka misstänkta transaktioner jämfört med privatkonton. Utöver svårigheten som följer av den högre komplexiteten finns även andra sårbarheter som bidrar till att företag kan missbrukas för olika typer av brottslighet. En sådan är kvalitetsbrister i registret över verkliga huvudmän. Det är relativt lätt för kriminella att hitta bulvaner och företagsmålvakter, även i andra EU-länder. En annan sårbarhet är brister i bankernas rutiner och kontrollsystem avseende företagskunder. Brottsbekämpande myndigheter har sett exempel på att företag bytt både ägare, företrädare och verksamhet utan att det uppmärksammas av banken där företaget är kund.

Transaktioner i form av överlåtelser av kommersiella fastigheter och fusioner, förvärv eller köp av företag uppgår till hundratals miljarder kronor i Sverige varje år och involverar inte sällan utländska investerare. Det kan röra sig om komplexa och svårgenomskådliga ägarstrukturer, något som kan skapa förutsättningar för att tillgängliggöra medel för sanktionslistade entiteter och kringgå sanktioner.

⁶² FATF:s rekommendation är att FN:s sanktionerna ska genomföras inom 24 timmar.

8.3 Ägande och kontroll döljs genom transaktionskedjor i flera led

Det finns sårbarheter i det finansiella systemet som kan utnyttjas för att dölja ägande och kontroll samt medels syfte. Transaktioner i flera led försämrar transparensen vad gäller konton och överföringar.

8.3.1 Avsaknad av motpartsuppgifter

Krav på vilken information som ska åtfölja överföringar av medel, såsom uppgift om motpart finns reglerat på EU-nivå.⁶³ Trots att kraven trädde i kraft redan 2017 saknas det fortfarande stöd i viktiga delar av svensk betalningsinfrastruktur för att hantera överföring av nödvändig information med automatik.⁶⁴ Bristerna handlar om avsaknaden av information om betalarens och betalningsmottagarens betalkontonummer och skapar förutsättningar för aktörer att dölja finansiella spår och försvårar såväl upptäckt som utredning av brottslighet.

8.3.2 Digitala tjänster och gränsöverskridande transaktioner

För finansiella företag som inte har eget tillstånd att tillhandahålla inlåningskonton samlas kundernas behållning på det finansiella företags klientmedelskonto i en bank. Det innebär att kunderna inte kan identifieras som kontohavare i konto- och värdefackssystemet Mekanismen.⁶⁵ Om sådana företag är registrerade utomlands står de inte heller under tillsyn och kontroll av svenska myndigheter.

Bland dessa finns företag som erbjuder snabba gränsöverskridande transaktioner. Tjänsterna tillhandahålls digitalt vilket innebär att identifiering måste ske på distans. Det går ofta snabbt att registrera sig som ny kund och det förekommer att nya kunder får tillgång till tjänsterna direkt, innan kundernas uppgifter hunnit kontrolleras. Tjänsterna riskerar därför att missbrukas för att dölja medel och transaktioner.

⁶³ EU-förordning 847/2015 trädde ikraft 2017-06-26 och ersattes per den 2024-12-30 av förordning 1113/2023.

⁶⁴ Transaktioner som går genom Bankgirot och dataclearingen. Finansinspektionen har förelagt Bankgirots svenska ägarbanker att åtgärda bristerna senast den 31 december 2026, se Finansinspektionens beslut med dnr 24-11564, 24-11565 och 24-11566.

⁶⁵ Mekanismen är en teknisk plattform där anslutna myndigheter kan få information om förekomst av konton och värdefack hos institut, samt fastställa identiteten på konto- och värdefacksinnehavare.

8.3.3 Risker med virtuella bankkonton

Möjligheten att använda virtuella internationella bankkonton utgör också en sårbarhet som kan missbrukas i brottsligt syfte. De virtuella kontonumren kan följa standarden för ett land men vara kopplade till ett faktiskt bankkonto i ett annat, vilket gör det möjligt att genomföra snabba internationella betalningar utan att varken det underliggande kontot, kontoutfärdaren eller det verkliga mottagarlandet framgår av transaktionen.

8.3.4 Många mellanhänder och korrespondentbanker, bland annat i tredje land

Vid gränsöverskridande banköverföringar där avsändaren och mottagaren är kunder i olika banker behandlas betalningen normalt via en korrespondentbank, vilket är en bank som erbjuder inlåningskonton och behandlar betalningar för andra bankers räkning. Gränsöverskridande överföringar omfattar ofta flera korrespondentbanker och transaktionskedjan blir längre till länder där svenska banker inte har egna inlåningskonton och för att överföra betalningar mellan olika valutor. Antalet korrespondentbanker har dock minskat under senare år.⁶⁶ Möjliga förklaringar till det kan vara striktare penningtvättsregelverk, men det kan också vara på grund av betaltjänstleverantörer som erbjuder billigare och snabbare betallösningar.

Även utanför det reguljära finansiella systemet förekommer långa transaktionskedjor som använder flera finansiella system. Inom Hawala är det exempelvis vanligt att använda sig av banktransaktioner, överföringar via betaltjänstföretag och digitala applikationer eller betalning med kryptovalutor.⁶⁷

8.3.5 Finansiering via alternativ betalningsinfrastruktur i tredje land

En trend i det globala finansiella systemet är att olika geografiska regioner inför egna betalningsinfrastrukturer i syfte att bland annat minska beroendet till andra länder. Det finns en risk att kringgående av sanktioner och finansiering av massförstörelsevapen kan ske via dessa alternativa betalningsinfrastrukturer.

Ryssland driver sedan 2014 betalningsmeddelandesystemet System for Transfer of Financial Messages (SPFS) som utvecklades efter att EU införde

⁶⁶ Riksbanken (2022). Gränsöverskridande betalningar i fokus.

⁶⁷ Finanspolisen informerar (2025). Penningtvätt i ett internationellt perspektiv.

sanktioner och landet stängdes av från det globala meddelandesystemet SWIFT. I SPFS deltar bland andra Kina och Iran. Genom SPFS kan Ryssland fortsätta bedriva handel och göra finansiella transaktioner trots sanktioner.⁶⁸ Sedan april 2022 publicerar inte den ryska centralbanken namn på användare av SPFS⁶⁹ och sedan juni 2024 är det förbjudet för företag inom EU att ansluta sig till SPFS samt att direkt eller indirekt medverka i transaktioner med företag som använder SPFS.⁷⁰ Under 2025 förekom uppgifter om att knappt 180 finansiella företag från 24 länder var anslutna till SPFS.⁷¹

Även Kina driver sedan 2015 ett eget betalningsmeddelandesystem Chinese Cross-Border Interbank Payment System (CIPS) som också har clearing- och avvecklingsverksamhet för betalningar i den kinesiska valutan renminbi. CIPS kan även användas av så kallade indirekta deltagare; finansiella företag i Kina och i andra länder som inte har öppnat konton hos CIPS men som innehar CIPS-bankidentifierare och anförtror direkta deltagare att hantera transaktioner via CIPS. Även flera ryska banker är anslutna till CIPS som indirekta deltagare.⁷² I slutet av 2025 hade CIPS 190 direkta och 1567 indirekta deltagare, varav 261 från Europa.⁷³ Kina är dessutom både Irans och Nordkoreas största handelspartner.⁷⁴

Det finns därmed en risk att SPFS och CIPS kan användas som kanaler för betalningar via avancerade upplägg och transaktionskedjor med korrespondentbanker som tolererar sanktionsrisken.⁷⁵

8.4 Finansiering genom illegal finansiell verksamhet, så kallad underground banking

⁶⁸ Riksbanken (2026). Betalningsrapport 2026.

⁶⁹ Federal Reserve Bank of New York (2023). Financial Sanctions, SWIFT, and the Architecture of the International Payments System.

⁷⁰ Se artikel 5a i rådets förordning (EU) 833/2014 om restriktiva åtgärder mot bakgrund av Rysslands åtgärder som destabiliserar situationen i Ukraina. Till dessa förbud finns ett antal undantag.

⁷¹ Middle East Monitor (2025). 25 countries join Russia's payment system as an alternative to SWIFT.

⁷² Federal Reserve Bank of New York (2023). Financial Sanctions, SWIFT, and the Architecture of the International Payments System.

⁷³ CIPS (2025). CIPS Participants Announcement No. 115.

⁷⁴ World Trade Organization (2024), Iran Exports, samt Reuters (2026) China's trade with North Korea rises 22% in January and February as ties improve.

⁷⁵ Se bland annat Atlantic Council (2026). Inside Tehran's toll booth.; U.S.-China Economic and Security Review Commission (2025). China's Facilitation of Sanctions and Export Control Evasion.; Atlantic Council (2024). The axis of evasion: Behind China's oil trade with Iran and Russia.

Medvetenheten om riskerna för att det finansiella systemet missbrukas för brottslighet bedöms ha ökat i samhället senaste åren. I takt med att många verksamhetsutövare förbättrar sina kontrollsystem ökar efterfrågan på möjliggörare som kan hjälpa kriminella aktörer att runda kontrollerna. Det finns också en risk att aktörerna vänder sig till rent illegal verksamhet som erbjuder tjänster utanför det reguljära finansiella systemet, så kallad underground banking.

Framväxten av organiserad brottslighet i Sverige har skapat ett behov och förmåga av att kunna hantera och tvätta brottsvinster i stor skala. Det bedöms ha bidragit till att det har etablerats en illegal finansiell infrastruktur som erbjuder tjänster inom exempelvis kontant- och guldhantering och växling till kryptotillgångar. Den infrastrukturen kan även nyttjas för annan brottslighet i syfte att till exempel finansiera massförstörelsevapen.

Aktörerna som tillhandahåller illegala finansiella tjänster är i olika grad och i något led beroende av den legala ekonomin och banksystemet för sin egen hantering. Även om aktörerna därmed lämnar vissa spår i det reguljära finansiella systemet är de mycket svåra att upptäcka. Det rör sig om komplicerade strukturer av olika nätverkskluster i flera olika länder.

8.5 Finansiering via kryptotillgångar

Kryptotillgångar är attraktivt för illegala syften eftersom det erbjuder högre grad av anonymitet än exempelvis banköverföringar och kortbetalningar. För varje ny transaktion skapas nya block i en blockkedja med information om var tillgången kom ifrån och var den fördes över till. Det gör transaktionen spårbar, men avsändare och mottagare är i praktiken anonyma.

Sanktionsundandragande aktiviteter bedöms numer vara den främsta drivkraften bakom illegal kryptovolym. Plånböcker som kopplas till Islamiska revolutionsgardets (IRGC) nätverk bedöms ha mottagit drygt 3 miljarder dollar under 2025. Kryptotillgångar används bland annat för anskaffning av produkter med dubbla användningsområden, men även för att understödja regionala militära styrkor och för oljehandeln. Aktörer kopplade till Nordkorea bedöms ha stulit kryptotillgångar till ett värde av mer än 2 miljarder dollar under 2025. Nästan 1,5 miljarder dollar stals vid ett enda tillfälle från kryptobörsen Bybit i februari 2025. Stölder av kryptotillgångar används för att finansiera prioriteringar av till exempel landets kärnvapenprogram, samt kringgå internationella sanktioner.⁷⁶

⁷⁶ Chainalysis (2026). Crypto Crime Report.

Stablecoins bedöms dominera den illegala kryptoaktiviteten.⁷⁷ Stablecoins ges ut av privata aktörer och erbjuds både på centraliserade och decentraliserade plattformar. Information om innehavare till konton och plånböcker finns inte hos utgivaren utan kan finnas hos plånboksleverantörer eller handelsplatser som exempelvis kryptobörser som oftast är den som har direktkontakt med slutkunden.⁷⁸ Även självförvaltande plånböcker som varken kopplas till en plånboksleverantör eller handelsplats används i stor utsträckning, där användaren själv kontrollerar sina tillgångar utan att någon extern aktör har insyn.⁷⁹

Införandet av MiCA-förordningen förväntas leda till en ökad transparens och förbättrad regel efterlevnad bland leverantörer av kryptotillgångstjänster inom EU. Trots detta öppnar den decentraliserade och globala handeln med kryptotillgångar upp för möjligheter att kringgå regleringar och använda kryptotillgångar i illegala syften. Mindre strikta kontroller och otillräckliga kundkännedomprocesser hos kryptoaktörer kan utnyttjas och tillåta aktörer att öppna konton med falska eller stulna identiteter för att genomföra transaktioner. Många kryptoaktörer, såväl utgivare som handelsplatser, har dessutom sitt säte utanför EU, vilket ytterligare begränsar svenska myndigheters möjligheter till tillsyn och åtgärder. En stor del av kryptoväxlarna är illegala aktörer som agerar utan tillstånd eller registrering. Illegala växlare kan i sin tur använda legala kryptoplattformar för sina transaktioner.

8.6 Finansiering genom försäljning av tjänster och arbetskraft

Ett sätt som framför allt den nordkoreanska regimen använder sig av för att generera intäkter som bidrar till landets program för massförstörelsevapen är genom försäljning av tjänster och arbetskraft.

Genom sofistikerade bedrägeriupplägg där tusentals skickliga nordkoreanska IT-arbetare under falska identiteter får anställningar eller säljer konsulttjänster genererar de inkomster till den nordkoreanska regimen.⁸⁰ Arbetarna beräknas tjäna mellan 3 500 – 10 000 dollar, i vissa fall upp till 100 000 dollar, per månad. Av detta får de behålla cirka 5–10 procent. Inkomsterna skickas vanligen via online-baserade penningöverförartjänster

⁷⁷ Chainalysis (2026). Crypto Crime Report.

⁷⁸ Till exempel Safello, BTCX, Trijo, Goobit.

⁷⁹ Riksbanken (2026). Betalningsrapport 2026.

⁸⁰ The U.S. Department of State, the U.S. Department of the Treasury, and the Federal Bureau of Investigation (FBI) (2022). Guidance on the Democratic People's Republic of Korea Information Technology Workers.

och genom krypto. Nordkoreanska regimen bedöms ha erhållit cirka 350 – 800 miljoner dollar under 2024 på detta sätt. IT-arbetarna arbetar främst i sektorer kopplade till försäkring och teknologi, men också inom artificiell intelligens, krypto och försvar. Nordkoreas fokus har, efter amerikanska myndigheters tillslag, skiftat till europeiska små och medelstora IT-företag. Utöver risken att finansiera massförstörelsevapen, riskerar dessa företag även dataintrång, intrång i immateriella rättigheter, stöld samt ekonomiska, juridiska och anseendemässiga skador.⁸¹

2024 fanns det uppgifter om att fler än 100 000 nordkoreanska medborgare arbetade i cirka 40 olika länder, vilket väntades öka avsevärt de närmaste åren.⁸²

8.7 Finansiering genom försäljning av varor

Risken för att utförsel av varor från Sverige används för att finansiera spridning av massförstörelsevapen bedöms generellt som låg, men den kan inte uteslutas. Legitima handelsflöden kan i vissa fall utnyttjas för att generera intäkter som direkt eller indirekt används för finansiering av massförstörelsevapen. Risken är särskilt relevant vid handel med högriskländer, komplexa leveranskedjor, användning av mellanhänder eller när den verkliga mottagaren av varorna är svår att identifiera. Sveriges exportkontrollsystem, tillsynsmyndigheter och krav på kundkännedom bidrar till att begränsa sårbarheterna. Samtidigt kan aktörer avsiktligt försöka kringgå regelverket genom falska dokument, bulvanupplägg eller omdirigering av varor vilket gör att en viss sårbarhet kvarstår.

⁸¹ Multilateral Sanctions Monitoring Team (2025). The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities.

⁸² United Nations Security Council (2024). S/2024/215.

9 Samlad bedömning

En jämförande bedömning av sju identifierade riskområden för finansiering av spridning av massförstörelsevapen redovisas i riskmatrisen nedan. Detta innebär att riskområdena endast bedöms och jämförs i relation till varandra. Rapporten gör därmed inte anspråk på att bedöma den samlade risken för finansiering av spridning av massförstörelsevapen i Sverige.

Bedömningen baseras på en samlad analys av de hot, sårbarheter och konsekvenser som har identifierats inom respektive riskområde. Vid riskvärderingen har bland annat regelverkets utformning, möjligheterna till tillsyn och kontroll, graden av transparens, verksamheternas omfattning samt geografiska och gränsöverskridande förhållanden beaktats. De olika riskområdena uppvisar betydande variationer avseende såväl exponering som möjligheter till upptäckt och riskreducerande åtgärder.

Inom den samlade bedömningen är den relativa risken högst inom illegal finansiell verksamhet, så kallad underground banking, samt genom användning av kryptotillgångar. Bedömningen motiveras främst av verksamheternas karaktär och omfattning, förekomsten av komplexa och gränsöverskridande transaktionsmönster samt möjligheten för aktörer att verka i parallella finansiella strukturer utanför den reglerade finansiella sektorn. Dessa omständigheter begränsar möjligheterna till insyn, försvårar upptäckt av otillåten verksamhet och minskar förutsättningarna för effektiva tillsyns- och kontrollåtgärder.

Den relativa risken bedöms vara lägst inom området försäljning av varor. Denna bedömning grundar sig främst på förhållandevis goda förutsättningar för tillsyn och kontroll, en hög grad av transparens samt begränsade indikationer på systematiskt missbruk i syfte att kringgå riktade ekonomiska sanktioner.

Tabell 1.



<u>Låg</u>	<u>Medel</u>	<u>Betydande</u>	<u>Hög</u>
Finansiering genom försäljning av varor.	Oförmåga och underlåtenhet att identifiera tillgångar och företag som ägs eller kontrolleras av sanktionslistade personer.	Ägande och kontroll döljs genom komplexa företagsstrukturer.	Finansiering genom illegal finansiell verksamhet, så kallad underground banking.
	Finansiering genom försäljning av tjänster och arbetskraft.	Ägande och kontroll döljs genom transaktionskedjor i flera led, inklusive via alternativ betalningsinfrastruktur i tredje land.	Finansiering via kryptotillgångar.

Sverige är, som tidigare nämnts, en öppen ekonomi med en relativt stor finansiell sektor samt en högteknologisk tillverkningsindustri och en, sett till sin storlek, stor försvarsindustri. Givet intresset från aktuella FN-sanktionerade stater att tillgodogöra sig medel eller anskaffa produkter, teknik och kunskap som kan vara av värde i ett massförstörelsevapenprogram krävs robusta strukturer för att identifiera försök att riktade ekonomiska sanktioner inte genomförs eller kringgås.

Finansiella aktörer, tillverkningsindustrin, exportföretag och berörda myndigheter behöver ha goda processer för att identifiera försök att genomföra dolda anskaffningar.