RISIKOVURDERING OM FINANSIERING AV SPREDNING AV MASSEØDELEGGELSESVÅPEN

Den sentrale enhet

Dokumentdato: 6. mai 2024

Innhold

Sammendrag

- Aktivitet i Norge knyttet til finansiering av spredning av masseødeleggelsesvåpen (MØV) vil hovedsakelig foregå på en indirekte måte gjennom kjøp av varer, tjenester og teknologi fra Norge eller ved kanalisering av midler via norsk finansiell infrastruktur.

- Aktører som forsøker å omgå regelverket bruker omfattende nettverk for å skjule midlenes opphav og destinasjon. Norske aktører kan uforvarende utnyttes og involveres i sanksjonsomgåelser.

- Enkelte sårbarheter for MØV-finansiering vil overlappe med sårbarheter for både hvitvasking og terrorfinansiering.

- En sentral sårbarhet ved risikoen for MØV-finansiering er begrenset oppmerksomhet på og kunnskap om ulovlig anskaffelsesvirksomhet og MØV-finansiering. Norske virksomheters evne og mulighet til å identifisere midlenes opprinnelse, mottaker eller reell eier av virksomheter i tredjeland gjør de sårbare for utnyttelse til omgåelser av eksportkontrollregelverket.

- Bankenes elektroniske systemer for screening av kunder og transaksjoner har sårbarheter som kan utnyttes til MØV-finansiering. Systemene fanger opp kjente entiteter, mens risikoen for MØV-finansiering ofte knyttes til entiteter som ikke er fanget opp av sanksjonsregimer. Flere systemer har også dårlig treffsikkerhet.

- Det digitale domenet medfører sårbarheter på grunn av sin kompleksitet og at det i praksis ikke føres tilsyn med internasjonale aktører innen betalingsformidling og formidling av virtuelle verdier.

Introduksjon

Innledning

Norske myndigheter er ansvarlige for å utarbeide risikovurdering av finansiering av masseødeleggelsesvåpen (MØV-finansiering), som et ledd i implementeringen av Financial Action Task Force (FATF) sine anbefalinger. Dette kommer som et tillegg til eksisterende risikovurderinger innen terrorfinansiering og hvitvasking, som utgis av Politiets sikkerhetstjeneste (PST) og Økokrim. Denne rapporten er utarbeidet på oppdrag fra Justis- og beredskapsdepartementet (JD).

Rapporten har til hensikt å styrke risikoforståelsen hos private og offentlige virksomheter i Norge som kan være eller bli utsatt for ulike trusselaktører sine forsøk på MØV-finansiering eller ulovlige anskaffelser til utvikling og produksjon av MØV og disses leveringsmidler.

Det er innhentet informasjon fra PSTs egne trusselvurderinger og relevante rapporter (PST, 2023, 2024). Informasjon fra Etterretningstjenestens (E-tjenestens) ugraderte trusselvurderinger Fokus 2023 og Fokus 2024 gir en god oversikt over det internasjonale bildet når det gjelder statlige aktørers utvikling og produksjon av MØV (E-tjenesten, 2023, 2024). I tillegg har Nasjonal sikkerhetsmyndighet (NSM) gitt innspill på kapittelet om sårbarheter. Rapporten peker også på nasjonale og internasjonale forpliktelser norske virksomheter har knyttet til ivaretagelse av sanksjonsregelverk og eksportkontrollbestemmelser.

Definisjoner

Masseødeleggelsesvåpen (MØV) er en fellesbetegnelse på våpensystem som har kjernefysisk, biologisk eller kjemisk våpenlast, og som kjennetegnes med stort skadeomfang, massedød og store materielle skader.

FATF definerer spredning av MØV som: "manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both dual-use technologies and dual use goods used for non-legitimate purposes)" (FATF, 2021).

FATF definerer videre MØV-finansiering som: "raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes)" (FATF, 2021).

Det er først og fremst statlige aktører som har kapasitet til og intensjon om å utvikle og produsere MØV. Begrepet «trusselaktør» kan derfor leses som statlige aktører.

MØV-finansiering kan også forstås som en stegvis prosess, med tre steg trusselaktøren går gjennom (Brewer, 2018a):

1. *Skaffe midler*. Gjennom trusselaktørens statsbudsjett, samt legitime eller illegitime kommersielle og kriminelle aktiviteter.
2. *Fordekke transaksjoner og midlenes opphav*. Sette opp finansielt nettverk, skall- og frontselskaper og fordekte eierskap, samt leveringsmetoder.
3. *Anskaffe varer, tjenester og teknologi*. Trusselaktøren skaffer tilgang til det internasjonale markedet for å betale for varer, tjenester og teknologi til utvikling og produksjon av MØV.

Internasjonal og nasjonal innsats mot MØV-finansiering

Financial Action Task Force (FATF)

FATF er et mellomstatlig organ som utarbeider anbefalinger innenfor hvitvasking, terrorfinansiering og MØV-finansiering. FATF har utarbeidet et rammeverk som setter internasjonale standarder innen motarbeidelse av økonomisk kriminalitet. Dette er standarder som er implementert globalt. Alle land blir gjennom omfattende landevalueringer rangert på etterlevelse og effektivitet i implementering av rammeverket. FATFs rammeverk innen MØV-finansiering er begrenset til etterlevelse av FNs sanksjoner mot Iran og Nord-Korea.

Som FATF-medlem har Norge forpliktet seg til rammeverket, og norske lover og regler innen økonomisk kriminalitet er betydelig påvirket av disse. For å oppfylle FATF-forpliktelsene har Norge et ansvar både nasjonalt og internasjonalt for å bidra i bekjempelsen av denne type økonomisk kriminalitet.

Arbeidet med en risikobasert tilnærming til innsatsen mot MØV-finansiering følger av FATF sine oppdaterte anbefalinger, som krever at land og private virksomheter identifiserer, vurderer, forstår og motvirker risiko for MØV-finansiering (FATF, 2023). For private virksomheter inkluderer dette et krav om å ha på plass et kontrollregime for å håndtere denne risikoen. Anbefalingene peker videre på viktigheten av å ha en nasjonal myndighet eller mekanisme som koordinerer innsatsen på området.

Nasjonal strategi mot hvitvasking, terrorfinansiering og finansiering av spredning av MØV

Regjeringens strategi mot hvitvasking, terrorfinansiering og finansiering av spredning av MØV peker på at arbeidet mot hvitvasking, terror- og MØV-finansiering skal være risiko- og kunnskapsbasert, og koordinert mellom aktørene (JD & FIN, 2020). En risikobasert

tilnærming vil si at man setter inn størst innsats og tiltak mot områder, sektorer og fenomen med størst risiko.

Strategien fremhever viktigheten av at private og offentlige aktører har et systematisk forebyggende arbeid på området for å motvirke de potensielt store skadevirkningene. De rapporteringspliktige er sentrale i dette arbeidet og utgjør førstelinjen i den nasjonale innsatsen.

Rapporteringspliktige er foretak og personer som er underlagt hvitvaskingsregelverket som består av hvitvaskingsloven og hvitvaskingsforskriften. I stort gjelder dette for banker og finansnæringen, i tillegg til blant annet revisorer, advokater og eiendomsmeglere.

Strategien peker på at det kreves mer kunnskap om fordekte transaksjoner hos kontrolletater, politi og finansnæring for å kunne avdekke MØV-finansiering, som ofte er godt fordekt. Strategien peker videre på at trusselen i Norge knyttet til spredning av MØV forekommer gjennom fordekte anskaffelser av materialer, teknologi og kunnskap. Dermed er det avgjørende at virksomhetene selv, finansnæringen og rapporteringspliktige samt andre myndigheter evner å avdekke forsøk på fordekte anskaffelser.

Norges etterretnings- og sikkerhetstjenester (EOS-tjenester) har et ansvar for risiko- og trusselvurderinger, som også omfatter MØV. PST skal forebygge og etterforske trusler mot nasjonens sikkerhet knyttet til spredning av MØV, utstyr, materiale og teknologi for produksjon av slike våpen samt overtredelser av bestemmelser i eller i medhold av eksportkontrolloven og sanksjonsloven. E-tjenesten varsler om ytre trusler mot Norge og allierte, inkludert hvordan trusselaktører utvikler sine MØV-kapasiteter. Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende sikkerhet. NSM skal anbefale tiltak og vurderer hvordan sårbarheter i norske virksomheter og samfunnsfunksjoner påvirker risikobildet i lys av trusselbildet som beskrevet av E-tjenesten og PST.

Internasjonale sanksjoner og det norske eksportkontrollregelverket

Relevant lovverk som regulerer eksportkontroll og MØV-finansiering omfatter eksportkontrolloven (Eksportkontrolloven, 1987), med forskrift og sanksjonsloven (Sanksjonsloven, 2021) med tilhørende forskrifter, som implementerer internasjonale sanksjoner og restriktive tiltak i norsk lov. FNs sanksjoner mot hhv. Iran (FN, 2006, 2007, 2008, 2010) og Nord-Korea (FN, 2006, 2009, 2013, 2013), som nevnt i FATFs anbefalinger, er implementert i forskrifter til sanksjonsloven. I tillegg implementeres EUs forordninger og restriktive tiltak Norge velger å slutte opp om i norsk lov gjennom forskrift til sanksjonsloven. Forordninger og restriktive tiltak mot Syria (Forskrift om restriktive tiltak mot Syria, 2011) og Russland (Sanksjonsforskrift Ukraina, 2014) samt restriktive tiltak mot spredning og bruk av kjemiske våpen er eksempler som er blitt implementert i norsk lov for å motvirke spredning og MØV-finansiering (Utenriksdepartementet, 2023a).

Personer som har bopel i Norge og norske selskaper, stiftelser og sammenslutninger kan ikke uten særskilt forhåndstillatelse drive handel med, formidle eller på annen måte bistå med salg eller yte finansiell bistand til entiteter utenfor Norge i tilknytning til varer eller teknologi som er omfattet av eksportkontroll og sanksjonsbestemmelser.

Eksportkontroll er et virkemiddel etablert for å redusere faren for at varer, tjenester og teknologi brukes på måter som kan true internasjonal sikkerhet. I Norge er det Utenriksdepartementet (UD) som forvalter det norske regelverket og som er faglig myndighet. Dette innebærer blant annet at UD vurderer juridiske og tekniske sider i søknader om utførselslisenser, og beslutter om en eksport kan gjennomføres eller ikke. Det er imidlertid den enkelte virksomhet selv som må kjenne til hvorvidt deres varer, teknologi eller tjenester omfattes av eksportkontrollregelverket. Overtredelser anmeldes til og etterforskes av PST (Politiloven, 1995, § 17 b).

Flerbruksvarer og flerbruksteknologi er sivile varer og teknologi som også kan ha militære bruksområder.

Hvitvaskingsloven og –forskriften (Hvitvaskingsregelverket)

Rapporteringspliktige i Norge har plikt til å rapportere om mistenkelige transaksjoner (MT-meldinger) i henhold til hvitvaskingsregelverket, som består av hvitvaskingsloven med forskrift (Hvitvaskingsloven, 2018). Enheten for finansiell etterretning (EFE) ved Økokrim, mottar MT-meldinger fra de rapporteringspliktige, og utarbeider beslutningsstøtte til norske myndigheter med bakgrunn i denne rapporteringen. For å sikre etterlevelse av hvitvaskingsregelverket må også tilsynsmyndighetene kunne vurdere risikoen for etterlevelse av lovverket, samt sårbarhetene til de rapporteringspliktige.

Hvitvaskingsregelverket omfatter kun plikter til innsats mot hvitvasking og terrorfinansiering, og inkluderer ikke plikter for de rapporteringspliktige til å sette inn en risikobasert innsats spesifikt mot MØV-finansiering.

Hvitvaskingsregelverket gir likevel noen muligheter for de rapporteringspliktige til å kunne avdekke MØV-finansiering gjennom undersøkelsesplikten. Den inntreffer om en transaksjon eller forhold ved en kunde avviker fra den rapporteringspliktiges kjennskap til kunden. Ved grunnlag om mistanke etter undersøkelser, skal det rapporteres til Økokrim.

Trusselbildet

Trusselaktører

PST vurderer at Russland og Kina er de mest fremtredende trusselaktørene i Norge hva gjelder anskaffelsesvirksomhet av varer, tjenester og teknologi til utvikling og produksjon av MØV og leveringsmidler til disse. PST forventer at Kina og Russland vil stå bak de fleste forsøkene på anskaffelser av varer, tjenester og teknologi på fordekte måter i Norge i det kommende året.

Russland vil fortsette å utgjøre den største kjernevåpentrusselen mot NATO, og dermed også Norge. Russisk konvensjonell militærmakt, og dens avskrekkingsevne, er betydelig svekket etter flere år med krigføring i Ukraina. Både strategiske og taktiske kjernevåpen er blitt viktigere for russisk avskrekking i lys av dette. Til tross for at Russland har tilsluttet seg kjemivåpenkonvensjonen opprettholder de også fokus på utvikling av biologiske og kjemiske våpen. Russland har tidligere brukt slike våpen for å bekjempe motstandere av regimet.

Et omfattende sanksjonsregime er iverksatt mot Russland. Norge har med noen nasjonale tilpasninger sluttet opp om EUs sanksjonspakker mot Russland siden annekteringen av Krim i 2014 og fullskala-invasjonen av Ukraina i 2022. Russland er imidlertid fortsatt avhengig av vestlig teknologi og kompetanse for å opprettholde og vedlikeholde militær evne. Russiske aktører fortsetter sin anskaffelsesvirksomhet og tilpasser sin modus operandi til de vestlige sanksjonene.

EFE har siden 2022 og utbruddet av krigen i Ukraina opplevd et økt fokus fra de rapporteringspliktige på mistenkelige forhold knyttet til sanksjoner og sanksjonsomgåelser relatert til Russland. (EFE ved Økokrim, 2022, 2023). Mistenkelige forhold kan være sammensatte og omfatte både sanksjonsomgåelser og hvitvaskingshandlinger.

Kinesiske myndigheter bruker strategien for militær-sivil fusjon for å styrke kinesisk militærmakt. Dette bidrar til å viske ut skillet mellom sivil og militær sektor, og medfører økt bruk av sivil teknologi i kinesiske militære kapasiteter. For eksempel er en stor andel av brytningsteknologien Kina søker å tilegne seg, flerbruksteknologi som i stor grad utvikles av kommersielle aktører i sivil sektor.[1] Kina har ambisjon om å etablere en robust og troverdig

[1] Forskning og utvikling av brytningsteknologier brukes for å modernisere og utvikle nye militære kapasiteter. Dette inkluderer forskning innen kunstig intelligens, kvanteteknologi, bio- og genteknologi og autonomi.

kjernefysisk triade[2] innen 2040, likeverdig i volum og kapasitet som russisk og amerikansk. Så langt holder Kina fast ved en ikke-førstebruksdoktrine for kjernevåpen.

I tillegg kan også andre stater av bekymring forsøke å anskaffe varer, tjenester og teknologi fra Norge som er relevant for utvikling og produksjon av MØV eller finansiering av denne. Dette inkluderer Iran, Pakistan og Nord-Korea.

Som en reaksjon på at USA brøt atomavtalen i 2018 og gjeninnførte sanksjoner mot Iran, varslet iranske myndigheter at de kom til å anrike større mengder uran og til en høyere prosent anrikning enn det som er nødvendig for produksjon av atomenergi. Iran har i dag teknologi, kompetanse og nok anriket uran til å fremstille kjernevåpen. Landet har også en rekke missiler egnet for levering av kjernefysiske stridshoder som kan nå hele Midtøsten og store deler av Europa. Regimet er underlagt omfattende FN-sanksjoner. Mye av testaktiviteten kan imidlertid skje under dekke av Irans sivile romprogram.

Pakistan bruker i dag betydelige ressurser på sitt kjernefysiske program. Formålet med våpenprogrammet er å opprettholde Pakistans evne til strategisk avskrekking.

For Nord-Korea er troverdig evne til kjernefysisk gjengjeldelse mot USA og Sør-Korea garanti for regimets overlevelse. Regimet utvikler også taktiske kjernevåpen tiltenkt regional avskrekking og krigføring. Nord-Korea gjennomførte en rekke missiltester i 2023. Regimet er underlagt omfattende FN-sanksjoner målrettet mot å begrense Nord-Koreas program for utvikling og fremstilling av MØV.

Virkemidler

Aktivitet i Norge knyttet til MØV-finansiering vil hovedsakelig foregå på en indirekte måte. Norge er ikke et finanssentrum med store finansielle institusjoner med tilliggende utenlandske filialer og like store eller tilgjengelige muligheter for å skjule transaksjoner. Norge er derfor ikke det foretrukne alternativet for aktører som leter etter metoder for MØV-finansiering.

De fleste anskaffelsessaker er karakterisert av et omfattende nettverk av virksomheter og mellomledd, som bidrar til å skjule hvem som egentlig finansierer transaksjonen. Aktørene er organisert i nettverk av stråselskaper og mellomledd for å skjule de reelle aktørene bak anskaffelsene. Virkemidler som falsk dokumentasjon, kompliserte selskapsstrukturer, strå- og frontselskaper og uoversiktlige leverandørkjeder, unaturlige fraktruter eller uvanlige betalingsbetingelser, benyttes.

Fremmede stater kan i tillegg benytte seg av oppkjøp og investeringer i norske virksomheter for å sikre seg ulike strategiske fordeler. Slike økonomiske virkemidler kan utgjøre en trussel når de sees i sammenheng med hverandre eller når det for eksempel er snakk om å kjøpe opp småbedrifter i forsvarsindustrien eller virksomheter som utvikler, produserer eller selger sivil teknologi som også kan ha militære bruksområder.

[2] En kjernefysisk triade består av interkontinentale ballistiske missiler fra land, strategiske ubåter med interkontinentale ballistiske missiler fra sjøen og strategiske bombefly fra luften.

Etter Russlands fullskala-invasjon av Ukraina er russiske bedrifter for alle praktiske formål utestengt fra å kjøpe europeiske virksomheter og deltagelse i kontraktprosesser. Store deler av Russlands valutareserver i utlandet er frosset. Restriksjoner på eksport, finansiering og oppgjør tvinger Russland til å benytte tredjeland i transaksjoner. Russiske aktører har etablert et stort antall nye selskap i Europa og Sentral-Asia for å understøtte teknologianskaffelser. Nye eierskapsstrukturer og lengre leveringskjeder gjør det krevende å avdekke om Russland er sluttbruker. Både Russland og Kina benytter i økende grad vestlige frontselskaper eller selskaper i europeiske land som mellomledd i anskaffelsesaktiviteten.

En norsk bedrift eksporterte i juli 2022 maritimt utstyr til Russland. Det norske selskapet ble i forkant frarådet å eksportere varene med advarsel om at det kunne være i strid med sanksjonsreglene. Da forskuddsbetalingen ble stanset fordi den kom fra en russisk bank, ble fakturamottager endret slik at transaksjonen ble gjennomført via et tyrkisk mellomselskap.

Varestrøm og finansiering kan følge to forskjellige spor. Det kan være egne ruter med stråselskap og mellomledd for varene, i tillegg til parallelle ruter med andre stråselskap og mellomledd for de finansielle transaksjonene. Aktørene er tilpasningsdyktige og flytter aktiviteten mellom land. PST har eksempler på at finansielle strukturer kan utnyttes av mellomledd for pengestrømmen uten at varestrømmen kan spores til samme land.

I et nordisk land på medio 2000-tallet etablerte et selskap flere bankkonti for utenlandsk valuta. Kontoene ble benyttet som mellomledd for transaksjoner fra Iran til tredjeland. En del av transaksjonene gikk til selskap i Norge, hvorav noen produserte eller solgte flerbruksteknologi. Det forelå sterk mistanke om at noe av midlene var relatert til MØV-finansiering.

Noe senere åpnet selskapet en konto i en norsk bank. Dette sammenfalt med økte bekymringer og tiltak fra myndigheter i det nordiske landet. Transaksjonsmønstrene observert i det andre nordiske landet ble gjenfunnet i bankkontoen opprettet i Norge. Den norske banken fant flere av transaksjonene som mistenkelige og stengte etter hvert den aktuelle kontoen på bakgrunn av dette.

Eksemplet illustrerer hvordan både selskap og finansinstitusjoner kan utnyttes som en kanal sannsynlig med hensikt å bistå i MØV-finansiering. Videre belyser eksemplet hvordan aktører involvert i MØV-finansiering tilpasser seg tiltak fra myndigheter og flytter aktiviteten over landegrenser etter hvert som mistanke fattes eller de blir avdekket.

Også bankkonti til privatpersoner involveres i MØV-finansiering. Privatpersoner med knytninger til land og aktører av bekymring engasjeres, enten frivillig eller under press, i både anskaffelser av varer og finansieringen av dette.

En iransk forretningsmann bosatt i Norge kontaktet flere leverandører av laboratoriemateriell i Norge. Personen arbeidet fulltid men drev også et lite import-eksportselskap fra hjemmeadressen sin.

Mannen bestilte en rekke produkter til bruk i biologiske laboratorier. Enkelte av produktene hadde restriksjoner mot eksport etter sanksjonsloven, mens andre var innenfor regelverket. Det ble ikke oppgitt informasjon om sluttbruker av produktene.

Forretningsmannen skulle betale for produktene fra egen privat bankkonto. Om transaksjonen hadde blitt gjennomført ville imidlertid utlegget vært større enn personen hadde kunnet dekke på bakgrunn av lønn og inntekter fra selskapet sitt. Aktiviteten ble varslet til norske myndigheter som avdekket at finansiell bidragsyter for anskaffelsene var en aktør med antatte knytninger til utvikling av biologiske våpen.

Muligheten til å bryte pengesporet ved bruk av kontanter benyttes, på lik linje som ved hvitvasking og terrorfinansiering, også i MØV-finansiering. I Norge er mange aktører involvert i sirkulasjonen av kontanter, noe som gjør at oversikten over kontantbruken er fragmentert. Økokrim peker på at det frem til sommeren 2023 ble smuglet i snitt rundt 27 mill. norske kroner i kontanter ut av landet hver dag, hvor man ikke kjenner til kontantenes destinasjon eller sluttbruk. Dette kan muliggjøre en omfattende bruk av norske kontanter i den kriminelle økonomien (Økokrim 2023).

En norsk forhandler selger høy-kvalitets dieselmotorer med en rekke anvendelsesområder – herunder militært. Denne forhandleren ble kontaktet av en bruktbilforhandler som oppga at han ønsket å kjøpe et mindre antall motorer til bruk i lokomotiver på vegne av et georgisk selskap.

Senere i forhandlingene ble typen motorer endret til maritime modeller og antallet ble endret. Endringene medførte mer avanserte produkter og deretter også en vesentlig økning i pris. I tillegg bestilte bruktbilforhandleren også flere ulike typer flerbruksteknologi som kan anvendes både sivilt og militært fra andre forhandlere.

Personen reiste i tillegg hyppig til utlandet og brakte kontanter tilbake til Norge fra disse reisene. Ved ett tilfelle deklarerte personen inn kontanter en dag, og overførte tilsvarende beløp fra sin private bankkonto til en europeisk forhandler av flerbruksvarer påfølgende dag. Over to år importerte personen nok penger til å dekke alle bestillinger utenom dieselmotorene.

Eksemplet illustrerer at mulighetsrommet i å handle med kontanter også brukes i MØV-finansiering. I dette tilfellet ble det etterhvert avdekket at sluttbruker ikke var et georgisk selskap, men alle ordrene var gjort var på vegne av en militær enhet i et annet land.

Trusselaktørene benytter også virtuell valuta for å finansiere anskaffelser, men omfanget er ukjent i Norge. Nord-Koreas tyverier av virtuell valuta for å finansiere landets kjernevåpenprogram er et eksempel på en fremgangsmåte som flere sanksjonerte stater kan tenkes å benytte seg av. Det er en økende global trend at sanksjonerte aktører bruker virtuell valuta og annen ny teknologi for å unngå internasjonale sanksjonsregimer. Virtuell

valuta kan benyttes og utnyttes for å erverve og/eller flytte verdier uten behov for fysisk tilstedeværelse i det utsatte landet. Neobanker er typiske «internettbanker» uten fysiske filialer. De tilbyr tjenester via internett eller via mobilapplikasjoner og muliggjør enkel opprettelse av kundeforhold i utenlandske foretak, samt gjennomføring av hurtige internasjonale overføringer.

Fellesnevneren for hvitvasking, terrorfinansiering og MØV-finansiering er misbruk av lovlige finansielle mekanismer og verktøy for å oppnå egen vinning og støtte kriminalitet eller virksomhet som bidrar til å undergrave demokrati og trygghet. Disse lovbruddene må også ses i sammenheng med annen alvorlig kriminalitet. Korrupsjon er dessuten en faktor som kan bidra til å lette både gjennomføring av primærlovbrudd, hvitvasking av utbytte samt finansiering av terror og MØV (JD og FD, 2020). Det er viktig å ha en særlig årvåkenhet for pengestrømmene fra land der det skjer vesentlig utbyttegenererende kriminalitet, eller hvor avdekkingsrisikoen er lav, for eksempel som følge av korrupsjon, eller til land som eksporterer til sanksjonerte land.

Trusselen for MØV-finansiering skiller seg likevel fra trusselen knyttet til hvitvasking og terrorfinansiering på flere områder (FATF, 2021). MØV-finansieringen kan komme fra legitime og illegitime kilder, og har ikke vinning som hovedformål. Dette gjør at utbyttet fra den kriminelle aktiviteten knyttet til MØV-finansiering ikke nødvendigvis behøver å bli hvitvasket tilbake i den hvite økonomien. At pengesporet kun går i en retning på denne måten, har likhetstrekk med terrorfinansiering. Samtidig vil både MØV-finansiering og hvitvasking ha til felles at aktørene søker å fordekke reelle rettighetshavere gjennom komplekse eierskapsforhold og transaksjonsmønstre (També & Owen, 2023).

Mål i Norge

Rapporteringspliktige

Blant de rapporteringspliktige aktørene i Norge er finansnæringen sårbare for å involveres i MØV-finansiering gjennom produktene og tjenestene som tilbys deres kunder. Bruk av korrespondentbanker for internasjonale transaksjoner utgjør også en risiko for MØV-finansiering, da banker må forsikre seg om at også disse har tilstrekkelige kontrollregimer. Både Finanstilsynet og Økokrim peker på at det er høy risiko knyttet til at banker blir utnyttet til hvitvasking (Økokrim & PST, 2022). Dette kommer av at bankene er den primære leverandøren av finansielle tjenester, har et bredt tjenestetilbud, et stort antall kunder og er tilgjengelige. Banker med stor internasjonal eksponering er utsatt for særlig høy risiko.

Andre rapporteringspliktige med høy risiko for hvitvasking er betalingsforetak og agenter for utenlandske betalingsforetak, tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta og valutavekslere. Videre pekes det på betydelig risiko knyttet til e-pengeforetak, eiendomsmeglere, advokater og regnskapsførere. Selv om dette er risiko knyttet til hvitvasking, kan de samme forholdene også bli benyttet til MØV-finansiering. At en lang rekke bransjer har høy identifisert risiko for hvitvasking viser at trusselaktører kan utnytte et bredt spekter av produkter og tjenester hos de rapporteringspliktige.

En kundes knytninger til stater av bekymring vil være en sentral indikator i å avdekke trussel for MØV-finansiering. Det samme gjelder knytninger til land som er kjent mellomstasjon eller land med svake kontrollregimer eller mangelfull eksportkontroll. De rapporteringspliktige må ha kunnskap om land som er forbundet med høyere risiko ifølge hvitvaskingsregelverket, både listeførte og ikke-listeførte land. Dette kan som eksempel være land identifisert av FATF på de to såkalte «grey list» og «black list», som er land hvor det er identifisert en høy risiko for økonomisk kriminalitet (FATF, 2024). Kundens statsborgerskap, oppholdssted, foretaksregistrering, eierskapsforhold eller midlenes opphav, er alle relevante forhold i vurderingen av geografisk risiko (Finanstilsynet, 2022).

Trusselaktører vil i større grad benytte tjenester og produkter i bedriftsmarkedet til MØV-finansiering enn privatmarkedet. Trusselaktørenes anskaffelser og MØV-finansiering utnytter

etablerte internasjonale handelsmekanismer, hvor utsatte forretningsområder er internasjonale overføringer, trade finance, og forhold knyttet til korrespondentbanker.

Innen trade finance-segmentet vil banken i større grad være involvert i transaksjonen og kunne kreve mer dokumentasjon fra partene, enn ved enkelttransaksjoner. Ved enkelttransaksjoner med utlandet vil det ikke være de samme dokumentasjonskravene eller detaljnivået overfor banken knyttet til det underliggende ved transaksjonen. En trusselaktør kan dermed søke å benytte seg av enkelttransaksjoner for å fordekke underliggende detaljer ved transaksjonen.

Trusselen knyttet til privatmarkedet vil være lavere, da industriell aktivitet og internasjonal handel som regel ikke går gjennom dette kundesegmentet (Brewer, 2018b). Bedriftsmarkedet er også bedre egnet til å fordekke reelle rettighetshavere, gjennom transaksjoner med juridiske personer (Økokrim & PST, 2022).

Andre virksomheter

En rekke norske virksomheter utvikler, produserer og selger varer og teknologi av interesse for fremmede stater. Produsenter og tilvirkere av flerbruksteknologi er trusselutsatt. Norske virksomheter må selv være oppmerksomme på om deres teknologi kan ha militær nytteverdi. Utviklingen bærer preg av at flere stater av bekymring i stadig større grad benytter flerbruksvarer og –teknologi i sine våpenprogrammer. Dette innebærer at et bredt spekter av norske og andre vestlige virksomheter kan bli utsatt for fremmede staters anskaffelsesforsøk.

Kunnskap fra teknisk-naturvitenskaplig forskning kan ofte brukes i militær utvikling og noen stater har sterk interesse av å utnytte tilgangen og fortrinnene ved norske universitets- og forskningsinstitusjoner. Både adgang til laboratorier, opplæring i bruk av instrumenter, tilgang på test- og produksjonsutstyr og den teoretiske kunnskapen er ettertraktet. Internasjonalt forsknings- og utviklingssamarbeid forblir en arena som gir tilgang til sensitiv informasjon.

Virksomheter i Norge som utvikler, produserer eller selger sensor- og deteksjonsteknologi, maritim teknologi, halvlederteknologi, rom- og satellitteknologi samt drone- og kommunikasjonsteknologi, vil være utsatte mål for anskaffelsesforsøk. Brytningsteknologier, som kunstig intelligens, maritim autonomi, bioteknologi og kvantedatamaskiner er også av interesse.

Sårbarheter

Oppdagelsesevne hos rapporteringspliktige

Rapporteringspliktige og deres analyseverktøy

De rapporteringspliktige skal ha rutiner for å sikre at internasjonalt vedtatte sanksjons- og tiltaksforskrifter følges. Banker kjøper inn elektroniske systemer for screening mot de ulike sanksjonslistene for å identifisere kunder og transaksjoner tilknyttet personer og enheter som er underlagt sanksjoner og restriktive tiltak gjennomført i norsk rett.

En sårbarhet knyttet til dette er imidlertid at sanksjonsscreening kun fanger opp kjente individer og grupper, mens risikoen for MØV-finansiering ofte kan knyttes til personer som ikke er fanget opp av sanksjonsregimet. Det er derfor av stor betydning for bekjempelsen av MØV-finansiering at de rapporteringspliktige har flere systemer for å avdekke dette.

Økonomiske frystiltak er en utbredt form for sanksjoner og bankene er underlagt flere sanksjonsregelverk på grunn av sin internasjonale virksomhet. Frystiltakene innebærer påbud om at listeførte midler eller formuesgoder skal fryses, og forbud mot å stille til rådighet eller gjøre tilgjengelig penger eller formuesgoder for vedkommende. Dette kan typisk innebære å sperre tilgang til en bankkonto og forvaltede midler, eller at en transaksjon blir stanset. Utenriksdepartementets frysveileder gir praktisk veiledning i etterlevelse av frysbestemmelsene. Den retter seg i stor grad mot finansforetak og andre

rapporteringspliktige, da det er disse som størst risiko for å komme i kontakt med listeførte enheter og personer. Den vil også være relevant for andre som driver internasjonal virksomhet (UD, 2023b).

Antallet sanksjonerte personer, grupper og selskaper øker imidlertid og har spesielt tiltatt etter Russlands invasjon av Ukraina. Det medfører økt press på bankenes screeningrutiner og -systemer, og økt sårbarhet for at det forsøkes gjennomført transaksjoner som er underlagt frysforpliktelse gjennom bankene.

I takt med at antallet listeføringer har økt har også antallet transaksjoner som utløser en alarm og som må vurderes manuelt av fagspesialister økt. Dette kan være utfordrende og krever at bankene har medarbeidere med fagkunnskap på sanksjonsområdet. Dersom bankene ikke har denne kompetansen eller disse ressursene representerer det en sårbarhet.

Finanstilsynet har gjennomført et tematilsyn for å se på bankenes etterlevelse av forpliktelser knyttet til screening, både på kundescreening og transaksjonsscreening. Undersøkelsene var både på reelle sanksjonsdata (umanipulerte data), og på data som skal etterligne listeførte aktører som forsøker å forbigå sanksjoner (manipulerte). Tematilsynet viste at flere banker har dårlig treffsikkerhet på sin kundescreening, med lav treffsikkerhet på reelle data, og svært lav treffsikkerhet på manipulerte data. Treffsikkerheten på transaksjonsscreening var også lav. Dette viser at bankene er sårbare for å beholde eller etablere kundeforhold med sanksjonerte og listeførte personer og entiteter, samt sårbare for å gjennomføre transaksjoner der transaksjonsinformasjon er manipulert. Treffsikkerheten er høyere hvor bankene har benyttet en kombinasjon av flere screenings-systemer (Finanstilsynet, 2023).

Tematilsynet eksemplifiserer også sårbarheten knyttet til variasjonen innenfor de rapporteringspliktiges kontroll- og rapporteringsregimer. De største bankene og rapporteringspliktige i Norge har store avdelinger som håndterer et bredt sett av trusler knyttet til økonomisk kriminalitet. Rapporteringspliktige med langt mindre tilgang på personell og ressurser vil ikke ha de samme forutsetningene for å avdekke eller kjenne igjen mistenkelige forhold. Samtidig vil et høyt volum av transaksjoner og kunder hos de største rapporteringspliktige øke sannsynligheten for at enkelte mistenkelige forhold forsvinner i mengden.

Et godt informasjonsgrunnlag er nødvendig for å kunne innrette tiltak hensiktsmessig. Registreringsregimer er gode tiltak for å øke oppdagelsesevnen og gi bedre informasjonsgrunnlag, men dersom det ikke er etablert mekanismer som gir oppdagelsesrisiko dersom man unndrar seg registrering, vil det være en sårbarhet. Enkelte sårbarheter for MØV-finansiering vil overlappe med sårbarheter for både hvitvasking og terrorfinansiering, da strukturelle forhold og sårbarheter i regulering og finansielle tjenester vil kunne utnyttes til flere typer økonomisk kriminalitet.

Virtuell valuta og digitale utfordringer

Digitalisering og det store antallet nye aktører som springer ut av FinTech-industrien, slik som neobanktjenester og vekslingsplattformer for virtuell valuta, fører til nye sårbarheter. Virtuell valuta er et digitalt og grensekryssende produkt der tjenestetilbyderen ikke har en tydelig tilknytning til ett enkelt land, kombinert med at vekslere og oppbevaringstjenester av virtuell valuta vurderes å ha en høy iboende risiko for hvitvasking, terror- og MØV-finansiering. Med dagens digitale løsninger og globale samhandling over internett er det utfordrende å holde oversikt og kontroll over selskaper som tilbyr finansielle tjenester i Norge. Ulike nyere betalingstjenester etterlater seg elektroniske spor som det kreves kunnskap om og analyseverktøy for å avdekke.

Det er en sårbarhet at det er internasjonale aktører innen betalingsformidling og formidling av virtuelle verdier som det i praksis ikke blir ført tilsyn med. Det foreligger heller ikke informasjon om disse har tilstrekkelige regimer for etterlevelse av lover og regelverk

etablert. Tilbydere i Norge av virtuelle veklings- og oppbevaringstjenester, samt e-pengeforetak som neobanker, er rapporteringspliktige.

Miksetjenester, som er en tjeneste som blander ulike personers virtuelle valuta for å vanskeliggjøre sporing, utgjør en særlig høy trussel innen bruken av virtuell valuta. Nord-koreanske og russiske cyberkriminelle har i stor grad blitt knyttet til bruken av miksetjenester (Økokrim 2022).

Generelt er det digitale domenet sårbart på grunn av sin kompleksitet. Dette medfører at det i realiteten er vanskelig eller ikke mulig å ha en oversikt over sårbarheter i egne systemer. Dermed vil det være ukjente sårbarheter som kan utnyttes, både til å skjule finansiering og til å generere finansiering.

Skallselskaper og reelt eierskap

Kompliserte eierstrukturer og uoversiktlige forsyningskjeder benyttes for å omgå vestlige eksportregelverk. Å avdekke og hindre transaksjoner som går til MØV-finansiering er derfor en stor utfordring. Ofte er slike transaksjoner fordekte og svært vanskelig å spore. Da forblir ofte avsender og/eller mottaker skjult og endelig formål ukjent. En sentral sårbarhet er derfor norske virksomheters mangelfulle evne til og mulighet for å identifisere midlenes opprinnelse, mottaker eller reell eier av virksomheter i tredjeland.

Manglende innføring av register som identifiserer reelt eierskap representerer en sårbarhet. På nasjonalt plan er Lov om reelle rettighetshavere vedtatt, men registeret er ennå ikke effektuert. Internasjonalt er det enighet om registerføring, men kravene er ikke harmonisert på tvers av de ulike jurisdiksjoner.

De siste årene har det vært en mangedobling av kinesiske organisasjoner og teknologisentre som er involvert i åpen og fordekt kunnskapsoverføring internasjonalt. Kina er Norges største samarbeids-partner innen teknologi-vitenskapelige forskningsprosjekter. Dette skaper et betydelig handlingsrom for at kinesiske aktører enten frivillig eller under press kan overføre norsk teknologi til kinesiske militærprogram.

Oppkjøp og investeringer

Oppkjøp og investeringer i norske virksomheter kan brukes for å dekke militære og teknologiske behov, for eksempel ved å kjøpe eiendom som er strategisk plassert i forhold til norske militære installasjoner, og for å sikre kontroll over varer, komponenter og verdikjeder som er av avgjørende betydning for utvikling og produksjon av MØV, leveringsmidler for disse eller annen avansert våpenutvikling.

Det finnes en rekke sårbarheter i dagens regelverk for oppkjøp og investeringer. NOU 2023-28 *Investeringskontroll – En åpen økonomi i usikre tider* har pekt på at den norske ordningen for å kontrollere direkteinvesteringer av hensyn til nasjonale sikkerhetsinteresser ikke fungerer på en god nok måte (NOU 2023: 28).

Selskapsøkonomi

Norske virksomheter innen en rekke bransjer og sektorer utvikler og produserer varer, tjenester og teknologi med sivile bruksområder som også kan brukes militært. Disse virksomhetene kan utnyttes av aktører som har militær sluttbruk som mål for anskaffelsesvirksomheten de driver. PST erfarer at spesielt små og mellomstore bedrifter og virksomheter, eller virksomheter med svak likviditet, er sårbare for denne typen anskaffelsesvirksomhet. Manglende kunnskap om eksportkontrollregelverket, trusselbildet og bruksområdene for varen som virksomheten utvikler, produserer eller selger er med på å øke sårbarheten.

Finansiering av forskning og utvikling

Norge legger stor vekt på verdien av og behovet for internasjonalt utdannings- og forskningssamarbeid, samt utvikling av ny teknologi innenfor næringslivet. Dette er en forutsetning for å fortsatt være en kunnskapsnasjon og for å bidra til å løse de store utfordringene verden står overfor.

Autoritære stater utnytter imidlertid aktivt akademisk samarbeid på måter som er i strid med både akademiske normer og norske sikkerhetsinteresser. I flere land er det nære bånd mellom den sivile forskningen og militære forskningsprogrammer. Forskningsopphold i utlandet blir brukt for å sikre seg nødvendig kunnskap til utvikling av våpenprogrammer og MØV. Autoritære stater legger til rette for dette ved å finansiere egne borgeres forsknings- og utvekslingsopphold og/eller prosjekter ved norske institusjoner og virksomheter. Det kan også være tilfeller der norske, offentlige forskningsmidler bidrar inn i disse prosjektene og dermed uforvarende bidrar inn i andre staters våpenprogram.

Svakheter i tilsynsvirksomhet og regulering

I FATFs landrapport og oppfølgingsrapporter har Norge en nåværende rangering på delvis etterlevelse av rammeverket på tre av FATFs 40 anbefalinger (FATF 2014, 2018, 2019a, 2019b, 2023). Det gjelder forhold knyttet til korrespondentbanker, transparens og reelle rettighetshavere, og statistikk. Manglende etterlevelse særlig innenfor rammeverket som angår korrespondentbanker og transparens og reelle rettighetshavere utgjør en økt sårbarhet for MØV-finansiering.

Rangeringen på korrespondentbanker har vedvart siden 2014 og peker på mangler i krav knyttet til norske finansinstitusjoners etablering av forhold til korrespondentbanker i utlandet.

Rangeringen på transparens og reelle rettighetshavere har også vedvart siden 2014. Manglende etterlevelse knyttet til reelle rettighetshavere skyldes i hovedsak at norske myndigheter ikke har god nok oversikt over utenlandske eiere i norske selskap. Proposisjon om reelle rettighetshavere åpner opp for en utrulling av et norsk register for reelle rettighetshavere som vil kunne adressere denne sårbarheten (Prop. 74 LS (2023-2024).

Norges rangering på effektivitet knyttet til implementering av målrettede sanksjoner innen MØV-finansiering ble oppgradert i FATFs oppfølgingsrapport i 2019 fra «Moderate» til «Substantial» (fra nivå to av fire, til nivå tre av fire). Oppgraderingen skyldes styrking av de rapporteringspliktiges etterlevelse av målrettede sanksjoner. Det gjenstår fortsatt moderate mangler innen monitorering av de rapporteringspliktiges kontrollregimer, samt at det pekes på et behov for sektorvis veiledning fra tilsynsmyndighetene. Videre pekes det på moderate mangler knyttet til de rapporteringspliktige som ikke er finansinstitusjoner, da innen tilsyn, implementering av sanksjoner, og manglende forståelse av plikter knyttet til sanksjoner.

Konklusjon

Risikoen for MØV-finansiering er kombinasjonen av ulike sårbarhets- og trusselfaktorer. Den kan være knyttet til brudd eller manglende implementering av målrettede finansielle sanksjoner, for eksempel som en følge av mangelfulle risiko- og kontrollsystemer i private og offentlige virksomheter, eller feiltolkning av regelverk. Disse sårbarhetene kan så utnyttes av ulike trusselaktører til å unngå målrettede sanksjoner, hvor et av virkemidlene kan være bruk av front- og skallselskaper eller mellommenn.

Sentralt i forsøkene på MØV-finansiering i Norge er fordekte transaksjoner ved anskaffelsesvirksomhet av varer, tjenester og teknologi fra norske virksomheter. Dermed er det avgjørende at virksomhetene selv, finansnæringen og rapporteringspliktige samt andre myndigheter evner å avdekke forsøk på fordekte anskaffelser.

Aktivitet i Norge knyttet til MØV-finansiering vil hovedsakelig foregå på en indirekte måte. Det er lite sannsynlig at Norge er det foretrukne alternativet for aktører som leter etter

metoder for å finansiere eller skaffe midler til anskaffelsesvirksomhet knyttet til spredning av MØV. Det er i stedet sannsynlig at statlige aktører først og fremst driver anskaffelsesvirksomhet av varer, tjenester og teknologi fra Norge.

Denne rapporten er ett bidrag til den nasjonale forståelsen av MØV-finansering. Andre nødvendige tiltak for å motvirke MØV-finansiering vil blant annet være et effektivt lovverk og reguleringer, offentlige og private virksomheters egne kontrollregimer og risikovurderinger, samt styrket offentlig-privat samarbeid på området. Det er også behov for mer kunnskap om fordekte transaksjoner både hos kontrolletater, eksempelvis skatt og toll, og politi og finansnæringen.

Litteraturliste

Brewer, J. (2017*). Study of Typologies of Financing of WMD Proliferation*. King's College London. Project Alpha.

Brewer, J. (2018a). *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation*. Center for a New American Security.

Brewer, J. (2018b*). The Financing of WMD Proliferation. Conducting Risk Assessments*. Center for a New American Security.

EFE ved Økokrim (2022). *Enheten for finansiell etterretning ved Økokrims årsrapport 2022*.

EFE ved Økokrim (2023). *Enheten for finansiell etterretning ved Økokrims årsrapport 2023*.

Eksportkontrolloven. (1987). Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. (LOV-1987-12-18-93).

Etterretningstjenesten (2023). *Fokus 2023.*

Etterretningstjenesten (2024). *Fokus 2024.*

FATF (2014). *Anti-Money Laundering and Counter-Terrorist Financing Measures. Norway. Mutual Evaluation Report.*

FATF (2018). *Anti-Money Laundering and Counter-Terrorist Financing Measures. Norway. 3rd Enhanced Follow-Up Report & Technical Compliance Re-Rating*.

FATF (2019a). *Anti-Money Laundering and Counter-Terrorist Financing Measures. Norway. Enhanced Follow-Up Report & 2nd Technical Compliance Re-Rating*.

FATF (2019b). *Anti-Money Laundering and Counter-Terrorist Financing Measures. Norway. Follow-Up Assessment.*

FATF (2023). *Anti-Money Laundering and Counter-Terrorist Financing Measures. Norway. Follow-Up Report & Technical Compliance Re-Rating.*

FATF (2024, 06. mai). "Black and grey" lists. http://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

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

FATF (2023). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.*

Finanstilsynet (2022). *Veileder til hvitvaskingsloven*. 4/2022. [Rundskriv].

Finanstilsynet (2023). *Rapport fra tematilsyn om sanksjonsscreening*.

FNs sikkerhetsråd (2006, 2007, 2008, 2010). FNs sikkerhetsråds resolusjoner nr. 1737, 1747, 1803 og 1929.

FNs sikkerhetsråd (2006, 2009, 2013, 2013). FNs sikkerhetsråds resolusjoner nr. 1718, 1874, 2087 og 2094.

Forskrift om restriktive tiltak mot Syria (2011). Forordning nr. 36/2012.

Hvitvaskingsloven (2018). Lov om tiltak mot hvitvasking og terrorfinansiering. (LOV-2018-06-01-23).

JD og FIN (2020). *Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen.* Justis- og beredskapsdepartementet og Finansdepartementet.

Meld. St. 15 (2023-2024). *Felles verdier – felles ansvar. Styrket innsats for forebygging og bekjempelse av økonomisk kriminalitet.* Justis- og beredskapsdepartementet.

NOU 2023: 28. (2023). *Investeringskontroll. En åpen økonomi i usikre tider.* Departementenes sikkerhets- og serviceorganisasjon.

PST (2023). *Nasjonal trusselvurdering 2023*.

PST (2024). *Nasjonal trusselvurdering 2024*.

Politiloven (1995). Lov om politiet § 17 b. punkt 3 og 4. (LOV-1995-08-04-53).

Prop. 74 LS 2023-2024. *Endringer i finansmarkedslovgivningen (samleproposisjon) og samtykke til godkjenning av fire beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av rettsakter på finansmarkedsområdet.* Finansdepartementet

Sanksjonsforskrift Ukraina (2014). *Forskrift om restriktive tiltak vedrørende handlinger som undergraver eller truer Ukrainas territorielle integritet, suverenitet, uavhengighet og stabilitet.* Forordning nr. 883/2014.

Sanksjonsloven. (2021*). Lov om gjennomføring av internasjonale sanksjoner*. (LOV-2021-04-16-18)

També, N. & Owen A. (2023). *Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide.* The Royal United Services Institute (RUSI).

UD (2023a). *Sanksjoner. Gjeldende sanksjoner og tiltak.* Utenriksdepartementet. https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/sanksjoner-og-tiltak1/sanksjoner-og-tiltak/id2008477/.

UD (2023b). *Finansielle sanksjoner: Veiledning om frysbestemmelsene.* Utenriksdepartementet.

Økokrim & PST (2022). *Nasjonal risikovurdering. Hvitvasking og terrorfinansiering 2022.*

Økokrim (2022). *Notat – miksetjenester*.

Økokrim (2023). *Nå er det NOK. Kontanter i den kriminelle økonomien*.