NATO UNCLASSIFIED

25. november 2020

DOKUMENT
AC/35-D/2002-REV5

JULGEOLEKUKOMITEE

NATO SALASTATUD TEABE JULGEOLEKU DIREKTIIV

Eesistuja kohusetäitja märkus

1. Käesoleva dokumendi lisas on dokumendi C-M(2002)49-REV1 „Turvalisus Põhja-Atlandi lepingu organisatsioonis“ (*Security Within the North Atlantic Treaty Organization*) täiendava NATO salastatud teabe julgeoleku direktiivi viies redaktsioon. See on olemuselt siduv ja kohustuslik. Käesolev dokument asendab dokumendi AC/35-D/2002-REV4, mis tuleks hävitada.

2. Käesolev redaktsioon kajastab NATO julgeolekupoliitika (*NATO Security Policy*, AC/35-N(2015)0025-AS1, 21. detsembri 2015. aasta redaktsioon) tervikliku läbivaatuse tulemusi.

3. Käesoleva dokumendi on heaks kiitnud julgeolekukomitee (AC/35-N(2020)0004-AS1, 4. novembril 2020) ning dokumendile rakendatakse korralist ülevaatamist.

(Allkiri) Marco Criscuolo

Lisa 1

Vastutav ametnik: M. Rožaj, NOS (Ext. 4084)

NATO SALASTATUD TEABE JULGEOLEKU DIREKTIIV
SISUKORD

Järgnevates direktiivi liidetes käsitletakse konkreetseid kordasid, kokkuleppeid ja näidisdokumente:

(a) LIIDE 1 – kulleritunnistus

(b) LIIDE 2 – juhised kullerile NATO salastatud teabe käsipostiga transportimiseks

SISSEJUHATUS

1. Julgeolekukomitee (AC/35) avaldab käesoleva NATO salastatud teabe julgeoleku direktiivi dokumendi C-M(2002)49 lisa E täiendusena. Direktiiv sisaldab kohustuslikke sätteid ja samuti nimetatud sätteid selgitavat teavet. Direktiivis käsitletakse seoses NATO salastatud teabega järgnevaid aspekte:

(a) salastatuse tasemed ja märgistamine;

(b) kontroll ja töötlemine;

(c) säilitamine;

(d) reprodutseerimine, väljavõtted ja tõlked;

(e) edastamine ja vedu;

(f) üleandmis-vastuvõtmisaktid ja arvestuse pidamine;

(g) kasutusest eemaldamine ja hävitamine ning

(h) turvaintsidendid.

NATO SALASTATUSE TASEMED, ERIKATEGOORIA TÄHISED, MÄRGISTUS JA ÜLDPÕHIMÕTTED

2. NATO salastatuse tasemed näitavad kui tundlik on NATO salastatud teave ja neid kohaldatakse selleks, et teavitada teabe saajat vajadusest tagada meetmed teabe kaitseks, mis oleksid kooskõlas kahju ulatusega, mis võib tekkida teabele volitamata juurdepääsu või teabe avalikuks tuleku puhul. NATO salastatuse tasemed ja nende tähendused on järgmised:

(a) COSMIC TOP SECRET (CTS) (TÄIESTI SALAJANE)
volitamata juurdepääs või avalikuks tulek tekitaks NATO-le erakordselt tõsist kahju;

(b) NATO SECRET (NS) (SALAJANE)
volitamata juurdepääs või avalikuks tulek tekitaks NATO-le tõsist kahju;

(c) NATO CONFIDENTIAL (NC) (KONFIDENTSIAALNE)
volitamata juurdepääs või avalikuks tulek tekitaks NATO-le kahju;

(d) NATO RESTRICTED (NR) (PIIRATUD)
volitamata juurdepääs või avalikuks tulek oleks kahjulik NATO huvidele või toimimisele.

3. Üksikasjalik juhend NATO salastatud teabe avaldajale selle kohta, kuidas määrata asjakohane NATO salastatuse tase erinevate valdkondade puhul NATO salastatuse tasemete salajasuse kahjustamise korral tekkiva mõju alusel on NATO salastatud teabe julgeoleku juhiste lisa 1 liites 1 (AC/35-D/1032, *Guidelines on the Security of NATO Classified Information*).

4. NATO UNCLASSIFIED teavet ja avalikkusele kättesaadavaks tehtavat teavet kaitstakse ja käideldakse kooskõlas NATO teabe haldamise põhimõtete (C-M(2007)0118, *NATO Information Management Policy*) ning NATO salastamata teabe haldamise dokumendiga (C-M(2002)60, *The Management of Non-Classified NATO Information*).

5. Mis tahes salastatud riiklikku teavet, mille NATO vastu võtab, kaitstakse kooskõlas NATO julgeolekupoliitikaga (*NATO Security Policy*) asjakohasel tasemel, mis on toodud riiklike tasemete vastavustabelis NATO salastatuse tasemete ja nende riiklike vastete dokumendi (AC/35-D/1002, *NATO Security Classifications with their National Equivalents*) lisas 1.

6. Erikategooria tähiseid kohaldatakse vastavalt määratletud NATO salastatud teabele, mis vajab hinnangute kohaselt täiendavat või tõhustatud kategoriseerimist, järgmiselt.

(a) ATOMAL on erikategooria teabele kohaldatav märgistus, mis näitab, et teavet kaitstakse kooskõlas Põhja-Atlandi lepingu osalisriikide tuumateabealase koostöö kokkuleppega (C-M(64)39, *Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic Information*) ja seda toetavate Põhja-Atlandi lepingu osalisriikide tuumateabealase koostöö kokkuleppe rakendamise halduskorraga (C-M(68)41, *Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMAL Information*);

(b) SIOP on erikategooria teabele kohaldatav märgistus, mis näitab, et teavet kaitstakse kooskõlas Ameerika Ühendriikide ühtse integreeritud tegevuskava (US-SIOP) teabe NATO-s töötlemise erikorra alusel (C-M(71)27(Revised), *Special Procedures for the Handling of United States Single Integrated Operational Plan Information within NATO*);

(c) CRYPTO on märgistus ja erikategooria tähis, mille abil tuvastatakse kõiki sidejulgeoleku (COMSEC) võtmematerjale, mida kasutatakse NATO krüptograafilise julgeolekuga seotud teavet kandvate kaugsidevahendite kaitsmiseks või autentimiseks; see näitab, et teavet kaitstakse kooskõlas asjakohaste krüptograafilist julgeolekut puudutavate põhimõtete ja direktiividega (SDIP-31/2 ja SDIP-293/1);

(d) BOHEMIA on märgistus, mida kohaldatakse erikategooria teabele, mis on saadud sideluurest (COMINT) või on sellega seotud. COSMIC TOP SECRET – BOHEMIA märgistusega teavet kaitstakse ranges kooskõlas NATO signaaliluure põhimõtetega (MC 101, *NATO Signals Intelligence Policy*) ja sellega kaasneva liitlaste ühenddoktriiniga (*Allied Joint Publication, AJP*), milles käsitletakse õpetuslikke ja protseduuriküsimusi.

7. NATO riigid ning NATO tsiviil- ja sõjalised organid kehtestavad meetmeid tagamaks, et NATO loodud või NATO-le avaldatud NATO salastatud teabele määratakse korrektne NATO salastatuse tase. NATO tsiviil- ja sõjaliste organite puhul hõlmavad meetmed järgmist:

(a) NS ja kõrgemal tasemel salastatud teabe NATO salastatuse taseme üle otsustamise volitused antakse piiratud arvule määratletud ametikohtadele;

(b) Salastamist vajava teabe hulka piiratakse ja tundlikum teave paigutatakse pigem tekstide liidetesse, et põhiteksti saaks kasutada laialdasemalt ja vähem rangeid turvameetmeteid kohaldades;

(c) dokumentidele tuleks määrata NATO salastatuse tase nendes sisalduva teabe põhjal, mis võib erineda nende dokumentide salastatuse tasemest, millele nimetatud dokumendid on lisatud, millele need viitavad või mille vastuseks need on koostatud ning

(d) NATO salastatud teave tuleb üle vaadata, et asjakohastel puhkudel salastatuse taset alandada või salastatus kustutada.

8. Avaldajad peaksid salastatuse tasemed iga viie aasta tagant üle hindama, et otsustada salastatuse taseme alandamise, salastatuse kustutamise ja lõpliku avalikustamise üle. Igal juhul vaadatakse üle NATO salastatud teabe salastatuse kustutamine ja avalikustamine 30 aasta möödudes (luure- ja tuumateabe puhul 50 aasta möödudes) kooskõlas NATO teabe avalikustamise põhimõtetega (C-M(2008)0116, *Policy for the Public Disclosure of NATO Information*).

9. Iga NATO tsiviil- ja sõjaline organ loob süsteemi tagamaks, et nende loodud CTS tasemel salastatud teave vaadatakse üle vähemalt iga viie aasta tagant ja NS tasemel salastatud teave vähemalt iga 10 aasta tagant, et veenduda, kas teabekandja salastatuse tase on endiselt põhjendatud. Ülevaatamine ei ole vajalik juhtudel, kui avaldaja on eelnevalt kindlaks määranud, et asjaomase NATO salastatud teabe salastatuse taset alandatakse automaatselt eelnevalt kindlaksmääratud perioodi möödumisel ning teave on ka vastavalt märgistatud.

10. Dokumendi üldine NATO salastatuse tase peab olema vähemalt nii kõrge kui selle osade kõrgeim salastatuse tase. Kaaskirjale märgitakse selle teabe kõrgeim NATO salastatuse tase, millele see on lisatud. Kaaskirja kasutamisel peab see sisaldama viidet, milles on selgelt välja toodud selle NATO salastatuse tase või märgistus juhuks, kui see eraldatakse lisadest, ning sellele tuleb tagada asjakohane kaitse.

11. Kui võimalik, siis peaks avaldaja edasist jaotamist puudutavate otsuste lihtsustamiseks märgistama asjakohaselt NR ja kõrgemal tasemel salastatud dokumentide lõigud, täiendused, lisad jne.

12. Iga dokumendi päisesse ja jalusesse märgitakse dokumendi kõrgeim NATO salastatuse tase. Dokumendi eraldiseisvatele lisadele/liidetele/manustele/täiendustele võib märkida kõrgeima NATO salastatuse tasemega võrreldes madalama salastatuse taseme.

13. Ilmselgete tegelikust salastatuse tasemest üle- või alasalastamise juhtumite puhul teavitab saaja sellest avaldajat. Kui avaldaja muudab dokumendi NATO salastatuse taset, teavitab ta sellest kõiki saajaid kirjalikult.

14. Avaldaja võib kohaldada lisamärgistusena NATO salastatud teabe edasise jaotamise piiramiseks juurdepääsupiirangu märgistust. Nimetatud administratiivsete või jaotamise piiramise märgistuste eesmärk on selgelt tuvastada dokumendis sisalduva teabe iseloom ja vajadus piirata juurdepääsu teabele.

Salastatud teabe kogumi põhimõte

15. Kui kokku on koondatud suur hulk NATO salastatud teavet, tuleb säilitada algsed salastatuse taseme märgistused ja hinnata, millist mõju avaldaks organisatsioonile teabekogumi kaotsiminek või salajasuse kahjustamine. Kui üldist mõju hinnatakse suuremaks kui NATO salastatuse tasemete tegelik individuaalne mõju, tuleks kaaluda teabe töötlemist ja kaitsmist tasemel, mis oleks kooskõlas teabe kogumi kaotsimineku või salajasuse kahjustamise hinnatava mõjuga.

NATO salastatuse tasemete muutmine või NATO salastatud teabe salastatuse kustutamine

16. NATO salastatud teabe salastatuse taset võib tõsta, alandada või salastatuse lõplikult kustutada ainult avaldaja või tema kirjalikul loal. Kui avaldajat ei ole võimalik tuvastada, võtab avaldaja vastutuse üle avaldaja õigusjärgne organisatsioon või kõrgem asutus. Sellistel juhtudel võib NATO salastatuse taset muuta või salastatust kustutada ainult pärast konsulteerimist NATO liikmesriikide või NATO tsiviil- või sõjaliste organitega, keda asjassepuutuv sisu mõjutab.

17. Kui NATO liikmesriigi või NATO tsiviil- või sõjalise organi avaldatud salastatud teave on ühendatud uueks kogumiks, ei või selle teabe salastatuse taset alandada ega salastatust kustutada ilma avaldaja kirjaliku nõusolekuta.

18. Avaldaja, või kui avaldajat ei ole võimalik tuvastada, siis tema õigusjärgne organisatsioon või kõrgem asutus vastutab saajate viivitamatu kirjaliku teavitamise eest, kui arvelevõtmise

kohustusega teabe[1] NATO salastatuse taset muudetakse või salastatus kustutatakse.

KONTROLL JA TÖÖTLEMINE

Registrisüsteem

19. Arvelevõtmise kohustusega teabe[2] vastuvõtmiseks, arvestuse pidamiseks, töötlemiseks, edastamiseks ja hävitamiseks tuleb pidada registrisüsteemi. Registrisüsteemi korrad ja nõuded kohalduvad ühetaoliselt nii füüsilises kui elektroonilises keskkonnas. Elektroonilist keskkonda puudutavad lisanõuded ja -teave on esitatud lisas F ja seda täiendavates direktiivides, nimelt: side- ja infosüsteemide julgeoleku põhidirektiivis (AC/35-D/2004, *Primary Directive on CIS Security*) ning side- ja infosüsteemide julgeoleku haldusdirektiivis (AC/35-D/2005, *Management Directive on CIS Security*). Registripidamise nõue võib olla täidetud nii ühe registriga, mille puhul tuleb CTS tasemel salastatud teavet alati rangelt eraldi hoida, või eraldi registrite ja kontrollpunktide loomisega.

(a) Iga asjassepuutuv NATO liikmesriik või NATO tsiviil- või sõjaline organ loob CTS tasemel salastatud teabele põhiregistri, mis toimib liikmesriigis või organis, milles see on loodud, peamise vastuvõtva ja saatva asutusena. Kui selleks on õiguspärane põhjus, võib liikmesriik põhiregistreid juurde luua (näiteks üks sõjalise ja üks tsiviilvaldkonna jaoks), aga nende arv tuleb hoida rangelt minimaalsena. Põhiregistrid võivad samuti tegutseda arvelevõtmise kohustusega muu teabe registritena.

(b) Registrid ja kontrollpunktid toimivad vastutava üksusena CTS ja NS tasemel salastatud teabe sisemisel edastamisel ja vastavas registris või kontrollpunktis hoitavate dokumentide üle arvestuse pidamisel; neid võib luua ministeeriumi, osakonna või väejuhatuse tasandil.

20. Kui registri personal, kes töötleb NATO liikmesriigis riiklikku salastatud teavet, on NATO salastatud teabele juurdepääsu saamiseks kohaselt kontrollitud ja töötlemise nõuetest informeeritud, võib selle personali ülesannetesse kuuluda ka vastutus NATO salastatud teabe eest.

Töötlemine registrisüsteemis

COSMIC TOP SECRET tasemel salastatud teave

21. CTS tasemel salastatud teavet, mida edastatakse teises NATO liikmesriigis asuvale adressaadile või NATO tsiviil- või sõjalisele organile, võib edastada ainult otse ühest registrist või kontrollpunktist teise, kui NATO liikmesriigi asjaomane asutus või NATO tsiviil- või sõjaline organ selleks loa annab.

22. Hoolimata registri tüübist tagavad CTS tasemel salastatud teavet töötlevad registrid COSMIC juhtiva ametniku (*COSMIC Control Officer*, CCO) nimetamise ja selle, et CCO määramisel arvestatakse registri koosseisu ja nõudeid. COSMIC juhtiva ametniku asetäitja (*Deputy COSMIC Control Officer*, DCCO) võib täita osa CCO ülesannetest ja võtab üle kõik volitused ja vastutuse CCO eemalviibimise korral.

[1] Kui liikmesriigid käsitlevad NC teavet arvelevõtmise kohustusega teabena, kohalduvad riiklikud õigusaktid.

[2] Arvelevõtmise kohustusega teave on dokumendis C-M(2002)49 määratletud kui CTS ja NS tasemel salastatud teave ning kogu erikategooria teave (näiteks ATOMAL).

23. COSMIC juhtiv ametnik (CCO) vastutab järgmiste ülesannete eest, mida võib delegeerida COSMIC registri juhile:

(a) kogu CTS tasemel salastatud teabe füüsiline kaitsmine, mida hoitakse põhiregistris, registris või kontrollpunktis, kuhu nad on vastutama määratud;

(b) registris või kontrollpunktis hoitava või seal ringleva või teistesse registritesse või kontrollpunktidesse edasi antava CTS tasemel salastatud teabe ajakohastatud arvestuse pidamine;

(c) tutvumislehtede ja hävitamise aktide üle arvestuse pidamine;

(d) ajakohastatud nimelise arvestuse pidamine nende isikute üle, kellele on antud juurdepääsuõigus registris või kontrollpunktis hoitavale CTS tasemel salastatud teabele;

(e) ajakohastatud arvestuse pidamine kõigi teiste registrite ja kontrollpunktide üle, kellega neil on lubatud CTS tasemel salastatud teavet vahetada, koos kõigi CCO-de nimede ja nende allkirjanäidistega;

(f) CTS tasemel salastatud teabe edastamine ainult nendele adressaatidele, kellel on juurdepääsuõigus CTS tasemel salastatud teabele;

(g) CTS tasemel salastatud teabe edastamine;

(h) edastatud või saadetud CTS tasemel salastatud teabe kohta üleandmis-vastuvõtmisaktide saamine;

(i) tagamine, et CTS tasemel salastatud teave tagastatakse vastutavale registrile kas säilitamiseks või hävitamiseks siis, kui seda enam ei vajata.

24. COSMIC põhiregistrite juhid teavitavad NATO julgeolekubürood oma vastutusala põhiregistrite või kontrollpunktide kõigist korralduslikest muudatustest.

25. Töötaja lahkumisest organisatsioonist tuleks registrit teavitada ühe kuu pikkuse etteteatamisega või tema organisatsiooni-sisesest üleviimisest kahe nädala pikkuse etteteatamisega selleks, et saaks korraldada inventuuri tema valduses oleva teabe üle. Kui talle ei ole määratud asendajat, võtab register tagasi ja säilitab töötaja vastutusel olnud NS või CTS tasemel salastatud teabe, kuni dokumendid saab üle anda.

26. Registrisüsteem kontrollib pidevalt CTS tasemel salastatud teavet ja peab arvestust iga dokumendi vastuvõtmise, edastamise ja hävitamise kohta. Arvestuses täpsustatakse COSMIC põhiregister, register, kontrollpunkt või isik, kelle valduses dokument on.

27. Vähemalt korra aastas viib iga register või kontrollpunkt läbi inventuuri kogu CTS tasemel salastatud teabe kohta, mille eest ta vastutab. CTS tasemel salastatud teave loetakse arvel olevaks, kui:

(a) see on füüsiliselt olemas, sisaldab õiget arvu lehekülgi ja sellel on õige eksemplarinumber;

(b) registrist või kontrollpunktist, kuhu see on üle antud, on saadud üleandmis-vastuvõtmisakt või

(c) dokumendi kohta on olemas NATO salastatuse taseme muutmise või salastatuse kustutamise teatis või hävitamise akt.

28. Registrid ja kontrollpunktid teavitavad iga-aastase inventuuri tulemustest vastutavat COSMIC põhiregistrit.

29. Vastutav julgeolekuasutus esitab kõigi COSMIC põhiregistrite iga-aastaste inventuuride tulemused NATO julgeolekubüroole hiljemalt iga aasta 31. märtsiks.

30. CTS tasemel salastatud teavet edastatakse COSMIC registrite kaudu. Registrid võivad edastada CTS tasemel salastatud teavet otse teistele registritele, kui edastamine ja vastuvõtmine registreeritakse teavet avaldavas ja vastuvõtvas registris. CTS tasemel salastatud teavet võib anda registrist või kontrollpunktist välja isikule, kes vastutab selle hoidmise eest, kuid teave tuleb tagastada, kui seda enam ei vajata. Isiku valduses olevat CTS tasemel salastatud teavet ei edastata muul viisil kui vastutava registri kaudu.

NATO SECRET tasemel salastatud teave

31. NS tasemel salastatud teabe töötlemise nõuded on järgmised:

(a) pidada ajakohastatud arvestust NS tasemel salastatud teabe üleandmise ja vastuvõtmise, edastamise ja hävitamise kohta;

(b) teha perioodilisi pistelisi kontrolle registri ja osakonna/isikute valduses oleva teabe kohta, veendumaks et teave on jätkuvalt nende kontrolli all.

NATO CONFIDENTIAL ja NATO RESTRICTED tasemetel salastatud teave

32. Kui riiklikes õigusaktides ei ole selgesõnaliselt nõutud teisiti, ei pea NC ja NR tasemel salastatud teave liikuma registrisüsteemi kaudu. NC ja NR tasemel salastatud teabele volitamata juurdepääsu tõkestamiseks tuleb rakendada asjakohaseid meetmeid.

SÄILITAMINE

33. NATO salastatud teavet säilitatakse kooskõlas dokumendi C-M(2002)49 lisaga D ja seda täiendava füüsilise julgeoleku direktiiviga. NATO salastatud teavet võib koguda või säilitada mis tahes vormis või teabekandjal, kui sellele kohaldatakse vastavalt salastatuse tasemele nõuetekohast kaitset. Mis tahes kogumile, mis sisaldab rohkem kui ühel NATO tasemel salastatud teavet, peab kohaldama kogumis sisalduvale kõige kõrgemale NATO tasemel salastatud teabele kohase kaitse.

KOOPIAD, VÄLJAVÕTTED JA TÕLKED

34. Saaja võib teha NS ja madalamal tasemel salastatud teabest koopiaid, väljavõtteid ja tõlkeid rangelt teadmisvajaduse põhimõtte alusel. Originaaldokumendi kohta kehtestatud turvameetmed kohalduvad ka selle väljavõtetele, koopiatele ja/või tõlgetele. NS tasemel salastatud teabe koopiad, väljavõtted ja tõlked märgistatakse identifitseerimiseks koopia järjekorranumbriga ja numbrid registreeritakse vastutavas registris. Saaja võib teha NC ja NR tasemel salastatud teabest koopiaid, väljavõtteid ja tõlkeid, kui need on sellise kontrolli all, mis välistab volitamata juurdepääsu. Mis tahes salastatud dokumendi väljavõttel on selle dokumendi või dokumendi osa (kui sel on individuaalne salastatuse tase) NATO salastatuse tase, millest väljavõte tehti. Kui väljavõtte NATO salastatuse tase on ebaselge, saadetakse kirjalik päring dokumendi avaldajale NATO salastatuse taseme korrektseks määramiseks.

35. Kõigile NATO salastatud töödokumentidele märgitakse kuupäev ja NATO salastatuse tase. Üksikisiku, allüksuse või osakonna koostatud NS tasemel salastatud dokumendi projekti, töödokumenti ja isiklikku väljatrükki (ja nende koopiaid) ei pea registreerima ega registri kontrolli all hoidma, välja arvatud juhul, kui need antakse välja avaldavast osakonnast või büroost, mistõttu avaldajad annavad vastutuse kaitsmise eest üle. Dokumendid tuleb aga arvele võtta maksimaalselt 5 tööpäeva jooksul pärast loomist. Kui neid on pärast selle tähtaja möödumist endiselt jooksvaks

tööks vaja, registreeritakse need registrisüsteemis ja antakse ametlikult isiku vastutusele.

36. Vajaduse korral ja kui on saadud avaldaja nõusolek, võib NATO salastatud teabe väljavõtteid lisada dokumentidesse, kui on kindlaks tehtud, et NATO liikmesriikides või NATO tsiviil- või sõjalistes organites tegutsevatel isikutel, kellel ei ole varem olnud juurdepääsuõigust NATO salastatud teabele, on teadmisvajadus. Sellistel asjaoludel peab asjaomastel isikutel olema asjakohane riiklik juurdepääsuluba, mis võimaldab juurde pääseda vähemalt sellisel riiklikul tasemel salastatud teabele, mis on selle väljavõtte NATO salastatuse taseme vaste.

37. Kui NATO salastatud dokumendi avaldaja soovib selles sisalduva teabe täiendavat edastamist kontrolli all hoida sätestab avaldaja nimetatud piirangud selgesõnaliselt märkes, näiteks: „Käesoleva dokumendi täielik või osaline reprodutseerimine ilma avaldaja loata on keelatud“ või „Lõikude … kuni …, lisade … ja … reprodutseerimine ilma avaldaja loata on keelatud“. Eripiiranguid tuleks kohaldada läbimõeldult ja nii harva kui võimalik. Täpsem juhend edastamismärgistuste kasutamise kohta on NATO salastatud teabe julgeoleku juhistes (AC/35-D/1032, *Guidelines on the Security of NATO Classified Information*).

38. Hoolimata avaldaja mis tahes kontrollipiirangutest või hoiatustest, kui dokument on vaja tõlkida NATO liikmesriigi keelde, säilitab tõlgitud dokument algse märgistuse, see peab vastama kõigile eespool toodud reprodutseerimise või väljavõtete tegemise kohta kehtivatele kriteeriumitele ja saama originaaliga samal tasemel kaitse. Kui CTS tasemel salastatud teavet on tarvis tõlkida, tuleb selleks saada avaldaja nõusolek.

39. CTS tasemel salastatud teavet ei reprodutseerita ning sellest ei tehta väljavõtteid, välja arvatud juhul, kui see on vajalik eespool kirjeldatud tõlke jaoks. Lisaks võib erandlikel asjaoludel teha CTS tasemel salastatud teabest erakorraliste missiooniülesannete täitmiseks paberkandjal koopiaid, väljavõtteid või tõlkeid, sealhulgas masinloetavate teabekandjate[3] jaoks mõeldud või neilt võetud väljavõtteid ja koopiaid, arvestades et:

(a) koopiad, väljavõtted või tõlked on saanud COSMIC põhiregistri COSMIC juhtiva ametniku (CCO) loa või selle edasivolitamise korral vastutava registri, allregistri või kontrollpunkti CCO loa;

(b) koopiatest, väljavõtetest või tõlgetest antakse teada COSMIC põhiregistrile, allregistrile või kontrollpunktile, mis peab arvestust tehtud koopiate arvu üle;

(c) koopiatel, väljavõtetel või tõlgetel on originaalteabe registreerimisnumber ja koopia järjekorranumber koos avaldaja ja reprodutseerinud COSMIC põhiregistri, allregistri või kontrollpunkti nimega;

(d) koopiad, väljavõtted või tõlked on märgistatud identifitseerimiseks koopia või tõlke teinud kohaliku asutuse määratud koopia järjekorranumbriga;

(e) koopiatel, väljavõtetel või tõlgetel on CTS salastatuse taseme märgistus ja kõik teised originaalteabe märgistused ning

(f) koopiad, väljavõtted või tõlked antakse COSMIC registri kontrolli alla, neid edastatakse COSMIC registri kanalite kaudu ja nende kohta antakse aru iga-aastases inventuuris koos muu CTS tasemel salastatud teabega.

[3] Masinloetav teabekandja on teabekandja, mis suudab edastada andmeid sensorseadmele.

40. Kui eespool sätestatud nõudeid ei saa viivitamatult täita operatsiooni või missiooniga seotud kriitilistel põhjustel, võib sidekeskuse[4] eest vastutav ametnik anda loa selliste koopiate ja tõlgete tegemiseks, mis on vajalikud CTS tasemel salastatud signaalide või sõnumite algseks edastamiseks. Koopiate ja tõlgete arvu üle peetakse arvestust ja koostatakse vastuvõtjate nimekiri. Seejärel vastutab signaalide või sõnumite reprodutseerimise ja tõlkimise eest COSMIC põhiregistri COSMIC juhtiv ametnik (CCO).

41. Operatsiooni või missiooniga seotud eesmärkidel võib saaja teha NS tasemel salastatud teabest koopiaid, väljavõtteid või tõlkeid, sealhulgas masinloetavate teabekandjate[3] jaoks mõeldud või neilt võetud koopiaid, kui koopiad, väljavõtted ja tõlked on märgistatud identifitseerivate koopia järjekorranumbritega ja koopiate ja/või tõlgete, sealhulgas koopiate arvu, registreerib vastutav register. Kui register ei ole kättesaadav, registreerib andmed saaja ja edastab need asjakohasele registrile esimesel võimalusel.

42. Inventari, sealhulgas reprodutseerimisseadmeid, faksimasinaid ning side- ja infosüsteeme, mis on lubatud ja akrediteeritud NATO salastatud teabe reprodutseerimiseks (või edastamiseks), peab füüsiliselt kaitsma, et neile omaks juurdepääsu ja neid saaks kasutada ainult volitatud isikud.

EDASTAMINE JA VEDU

43. Turvalisuse tagamise eesmärk edastamise ja füüsilise veo ajal on tagada asjakohane kaitse volitamata vaatluse, muutmise või (tahtliku või tahtmatu) avalikuks tuleku eest.

Edastamine

44. NATO salastatud teavet edastatakse teadmisvajaduse alusel. NC ja kõrgemal tasemel salastatud teavet edastatakse ainult isikule, kellel on asjakohasel tasemel juurdepääsuluba, kellele on tutvustatud tema julgeolekualaseid kohustusi ja kes on volitatud sellisele teabele juurde pääsema. Lisaks eespool loetletud nõuetele peab CTS tasemel salastatud teabe edastamine olema kooskõlas eespool toodud lõigetega 21 ja 30. NR tasemel salastatud teavet võib edastada isikutele, keda on teavitatud selleks ettenähtud kontrollimeetmetest, kellele on tutvustatud nõudeid ja kellel on ametlikel eesmärkidel teadmisvajadus.

Vedu

45. Käesoleva direktiivi kontekstis tähendab „teabe vedu“ NATO salastatud teabe füüsilist liigutamist ühest punktist teise punkti või rohkematesse punktidesse. NATO salastatud teabe transport veosena on lisaks reguleeritud salastatud projektide ja tööstusjulgeoleku direktiiviga (*AC/35-D/2003, Directive on Classified Project and Industrial Security*).

46. Üldpõhimõte on igal võimalikul juhul eelistada NATO salastatud teabe füüsilisele edastamisele turvaliste elektrooniliste vahendite kasutamist. Kõik side- ja infosüsteemid, millega töödeldakse NATO salastatud teavet, peavad läbima akrediteerimise kooskõlas dokumendi C-M(2002)49 lisaga F ja seda täiendavate direktiividega.

[4] Sidekeskus on infoliikluse käitlemise ja juhtimise eest vastutav organisatsioon, mis tavaliselt koosneb sõnumikeskusest, krüptograafiakeskusest ning edastamise ja vastuvõtmise jaamadest.

Käsipost

47. NATO või liikmesriigi töötajal, kes on määratud NC ja kõrgemal tasemel salastatud teavet käsipostiga kohale toimetama[5], peab olema asjakohase riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutuse (NSA/DSA) või muu pädeva julgeolekuasutuse antud juurdepääsuõigus. Nimetatud töötajat teavitatakse NATO julgeolekunõuetest ja juhendatakse nende kohustuste osas neile usaldatud NATO salastatud teabe kaitsmisel.

Kullerid / julgestus / saatjad

48. Kui NATO salastatud teabe edastamiseks on tööle võetud isikud julgestuseks ja saatjateks või olukorras, kus neil võib olla tahtmatult või volitamata juurdepääs NATO salastatud teabele, peavad nad olema läbinud julgeolekukontrolli sellisel tasemel, mida asjakohane julgeolekuasutus sobivaks peab.

Vedu NATO liikmesriigi asutuse või NATO tsiviil- või sõjalise organi asukoha või asutuse piires

49. NATO salastatud teave, mida transporditakse asukohta või asutuse perimeetris, peab olema kaetud, et takistada selle sisu vaatlemist. Sisekorrad, milles on määratletud asjakohased julgeolekunõuded, tuleks kehtestada ka juhul, kui NATO salastatud teavet transporditakse väljapool I või II klassi turvaala, näiteks administratiivaladel.

Vedu NATO liikmesriigi piires väljapoole NATO liikmesriigi asutust või NATO tsiviil- või sõjalise organi asukohta või asutust

50. Kui NATO salastatud teavet saadetakse asukoha või asutuse piirest väljapoole, tuleb järgida lõigetes 51 ja 52 toodud pakendamisnõudeid ning lõigetes 63 kuni 68 toodud üleandmise ja vastuvõtmise nõudeid. NATO salastatud teabe füüsiline edastamine NATO liikmesriigis toimub järgnevatel viisidel.

(a) **Sõjaline või riiklik kullerteenus**
kasutatakse CTS ja kõrgemal tasemel salastatud teabe puhul. MÄRKUS: see on ainus lubatud CTS tasemel salastatud teabe edastamise viis.

(b) **Riiklik postiteenus**
Kui see on riiklike õigusaktidega lubatud ja kui riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutus (NSA/DSA) või muu pädev julgeolekuasutus selle heaks kiidab, siis võib kuni NS tasemel (kaasa arvatud) salastatud teavet edastada riikliku postiteenusega.

(c) **Kommertskullerteenus**
Kui see on lubatud riiklike õigusaktidega ja kui riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutus (NSA/DSA) või muu pädev julgeolekuasutus selle heaks kiidab, siis võib sellist teenust kasutada kuni NS tasemel (kaasa arvatud) salastatud teabe edastamiseks.

(d) **Käsipost**
Kui see on riiklike õigusaktidega lubatud, siis võib kuni NS tasemel (kaasa arvatud) salastatud teavet edastada käsipostiga ka töötaja või lepinglane**, kes tegutseb kullerina** ning kellel on asjakohasel tasemel juurdepääsuluba tingimustel, mis on vähemalt sama ranged kui on ette nähtud NATO salastatuse tasemele, mis on vastava riikliku teabega võrdväärsel tasemel, arvestades et:

(i) asjakohases registris, kontrollpunktis või büroos peetakse arvestust kogu transporditava arvelevõtmise kohustusega teabe üle;

[5] Käsipost tähendab teabe edastamist nii, et isik kannab seda endaga kaasas.

(ii) NATO salastatud teave pakendatakse kooskõlas lõigetes 51 ja 52 toodud nõuetega ning lukustatud kohver või muu heakskiidetud pakend peab olema sellise suuruse ja kaaluga, et kuller suudab seda enda valduses hoida;

(iii) kuller hoiab NATO salastatud teavet enda otseses valduses, välja arvatud juhul, kui seda säilitatakse kooskõlas sätestatud turvanõuetega, seda ei jäeta järelevalveta ja seda ei avata teekonna vältel;

(iv) NATO salastatud teavet ei loeta avalikes kohtades;

(v) kullerile tutvustatakse tema julgeolekualaseid kohustusi ja talle antakse ametlik kirjalik luba vastavalt riiklikele õigusaktidele ning

(vi) NATO tsiviil- ja sõjaliste organite jaoks on NC ja NS tasemel salastatud teabe käsipostiga kohale toimetamine lubatud ainult erandlikel asjaoludel (nt kui isikutel on vaja reisida lühikese etteteatamisega, kui ajaliselt ei ole võimalik sellist teavet heakskiidetud turvaliste vahenditega saata või kui vastuvõtvas asukohas koha peal ei ole võimalik koopiaid teha). Isikutele, kes transpordivad NC ja NS tasemel salastatud teavet antakse NATO kulleri tunnistus (liites 1 on toodud kulleritunnistuse näidis).

51. NC ja kõrgemal tasemel salastatud teave, mida edastatakse ühest asukohast või asustusest teisele, tuleb pakendada nii, et see on kaitstud volitamata või tahtmatu avalikuks tuleku eest. Tuleb järgida järgmisi standardeid:

(a) see peab olema kahe läbipaistmatu ja tugeva pakendi sees; NS ja CTS salastatuse tasemete puhul võib lugeda välispakendiks avamist tuvastada võimaldavat turvaümbrikku, lukustatavat kotti, lukustatavat kasti või pitseeritud diplomaatilise posti kotti;

(b) sisepakend peab olema turvaline, sellele peab olema märgitud asjakohane NATO salastatuse tase ja muud ettenähtud märgistused ja hoiatused ning sellel peab olema vastuvõtja täisnimi, ametikoht ja aadress;

(c) välispakendil peab olema ettenähtud vastuvõtja nimi, ametikoht ja aadress ning üleandmis-vastuvõtmisakti jaoks kohaletoimetamise kinnituse kontrollriba;

(d) välispakend ei tohi viidata pakendis oleva sisu NATO salastatuse tasemele ning sellelt ei tohi selguda, et pakend sisaldab NATO salastatud teavet;

(e) kui NATO salastatud teavet toimetab kuller kohale käsipostiga, siis välispakendile peab olema selgelt märgitud „By Courier Only“ („Ainult kulleriga“).

52. NR tasemel salastatud teavet võib edastada minimaalselt ühekordses läbipaistmatus ümbrikus või pakendis. Pakendi märgistusest ei tohi selguda, et see sisaldab NR tasemel salastatud teavet.

Edastamine ühe NATO liikmesriigi territooriumilt teisele

53. CTS tasemel salastatud teavet edastatakse rahvusvaheliselt diplomaatilise posti kotis, riikliku kulleri või sõjalise kulleriga.

54. Kuni NS tasemel (kaasa arvatud) salastatud teavet edastatakse rahvusvaheliselt diplomaatilise posti kotis, riikliku kulleri, sõjalise kulleri või käsipostiga.

55. Kuni NS tasemel (kaasa arvatud) salastatud teabe edastamiseks võib kasutada riiklikke postiteenuseid, kui asjakohaste riikide riigi julgeoleku volitatud esindajad / määratud julgeolekuasutused (NSA/DSA) on sõlminud selliseks edastuseks asjakohase kahepoolse kokkuleppe.

56. Kommertsteenuseid võib kasutada kuni NC tasemel (kaasa arvatud) salastatud teabe edastamiseks, kui kommertsteenuse pakkuja on saanud selleks otstarbeks riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutuse (NSA/DSA) heakskiidu. Vastuvõtjat tuleks sellisest kohaletoimetamisest ette teavitada. Miinimumnõudena peab kommertsteenus andma võimaluse jälgida saadetise teekonda saatja juurest vastuvõtja juurde ja andma saatjale kohaletoimetamise kinnituse.

57. NATO salastatud teavet, mida edastatakse salastatud lepingute või programmide raames, võib edastada muude vahenditega kooskõlas dokumendi C-M(2002)49 lisaga G ja seda täiendava direktiiviga.

58. Muu posti- või kommertsteenuse kasutamisel peab pakendamisnõuete puhul järgima eespool lõigetes 51 ja 52 kirjeldatud üksikasju.

59. Kui NC ja kõrgemal tasemel salastatud teavet transpordib käsipostiga NATO või liikmesriigi määratud töötaja, siis tuleb järgida järgmiseid nõudeid:

(a) pakendil peab olema ametlik tunnusmärk või see peab olema pakendatud nii, et oleks üheselt mõistetav, et tegemist on ametliku saadetisega ja et see ei peaks läbima tolli- või turvakontrolli. Ametlikke liikmesriigi või NATO tunnusmärke tuleb töödelda kui arvelevõtmise kohustusega dokumente ja seega kaitstakse neid nagu NS materjali;

(b) kulleril peab olema kulleritunnistus, mida tunnustavad kõik NATO liikmesriigid (liites 1 on toodud nimetatud tunnistuse blankett), milles on tuvastatud pakend ja isiku luba pakendit transportida. Miinimumnõudena peab kullerit olema teavitatud vastavalt liitele 2;

(c) kulleri reisikorraldus peab olema kooskõlas järgnevate sihtkohta, teekonda ja transpordivahendeid puudutavate piirangutega või kui riiklikud reeglid on rangemad, siis kooskõlas riiklike reeglitega:

(i) kuller ei reisi riikidesse, mis ei kuulu NATO-sse, samuti mitte neist läbi ega üle nende ega kasuta mis tahes transpordivahendit või veoettevõtet, mis on registreeritud NATO-sse mitte kuuluvas riigis, mille kohta kehtib ükskõik milline allpool loetletud kriteeriumidest:

(1) riigi valitsus:

i. on sõnas või teos väljendanud vaenulikku suhtumist NATO ja/või NATO liikmesriikide suhtes;

ii. ei suuda tagada oma elanikele ja/või väliskülalistele üldiselt kokku lepitud inimelu ja/või isikliku vara kaitset või

iii. on tõendanud, et ei austa järjepidevalt diplomaatilise tunnusmärgi puutumatust;

(2) riigi luureteenistus on võtnud sihtmärgiks NATO ja/või NATO liikmesriigi;

(3) riik on sõjas või seal toimub tõsine tsiviilkonflikt.

60. Erandlikel juhtudel võivad riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutus (NSA/DSA) või NATO tsiviil- või sõjaliste organite juhid või nende määratud esindajad eespool lõike 59 punktis c sätestatud piirangutest loobuda, kui erakorralisi operatiivnõudeid ei ole võimalik muul viisil täita.

Vedu väljapoole NATO liikmesriikide territooriumit

61. Kuni NS tasemel (kaasa arvatud) salastatud teavet edastatakse NATO liikmesriikide territooriumilt väljapoole diplomaatilise posti kotis, riikliku kulleri, sõjalise kulleri või käsipostiga.

Infoedastus side- ja infosüsteemide kaudu

62. Kõik side- ja infosüsteemid, millega töödeldakse NATO salastatud teavet, peavad läbima akrediteerimise kooskõlas NATO julgeolekupoliitika (*NATO Security Policy*) lisaga F ja seda täiendavate direktiividega.

ÜLEANDMIS-VASTUVÕTMISAKTID JA ARVESTUSE PIDAMINE

63. Üleandmis-vastuvõtmisaktid on nõutavad pakendite puhul, mis sisaldavad NATO arvelevõtmise kohustusega teavet, mida edastatakse ühest asukohast või asutusest teisele, riigi territooriumi piires või rahvusvaheliselt. Üleandmis-vastuvõtmisakt saadakse pakendi numbri vastu. Üleandmis-vastuvõtmisaktid ei ole nõutud pakendite puhul, mis sisaldavad NC või NR tasemel salastatud teavet, välja arvatud juhul, kui avaldaja seda nõuab või kui see on selgesõnaliselt nõutav riiklike õigusaktide alusel. Üleandmis-vastuvõtmisaktid ei ole salastatud ja sisaldavad dokumendi registreerimisnumbrit, koopia järjekorranumbrit, dokumendi keelt ja lühipealkirja, kui see on salastamata.

64. Üleandmis-vastuvõtmisakt lisatakse CTS ja NS tasemel salastatud teavet sisaldava pakendi sisepakendisse. CTS ja NS tasemel salastatud teabe vastuvõtmine ja elukäik registreeritakse vastavalt käesolevas direktiivis sätestatule.

65. Üleandmis-vastuvõtmisakt, milles on loetletud dokumendid, tagastatakse viivitamatult saatjale, kui vastuvõttev register on lisanud sellele kuupäeva ja allkirja. Dokumendile, mis sisaldab arvelevõtmise kohustusega teavet, kirjutab alla ainult asjakohase juurdepääsuõigusega töötaja.

66. CTS tasemel salastatud teavet ja erikategooria teavet silmas pidades kirjutavad seda liiki arvelevõtmise kohustusega teabe üleandmis-vastuvõtmisaktile alla vaid COSMIC juhtiv ametnik (CCO), COSMIC juhtiva ametniku asetäitja (DCCO) või DCCO asendaja. Lisaks võib CTS tasemel salastatud teavet sisaldava pakendi sisepakendil olla märgistus, mis näitab, et seda tohib avada ainult konkreetne isik või büroo. Pakend tuleb aga avada CCO, DCCO või DCCO asendaja juuresolekul ja üleandmis-vastuvõtmisaktist või muust identifitseerimisinfost tuleb teha koopia, et dokumendi saaks kanda registrisüsteemi.

67. CTS tasemel salastatud teabe edastamiseks on nõutav järjepidev üleandmis-vastuvõtmisaktide kord. CTS tasemel salastatud teabe kasutajad kirjutavad tutvumislehele alla ja lisavad sellele kuupäeva ning see jääb dokumendi või toimiku külge kuni selle hävitamiseni. Tutvumislehte säilitatakse 10 aastat pärast dokumendi hävitamist.

68. NS tasemel salastatud teabe edastamiseks NATO liikmesriikides ning NATO tsiviil- ja sõjalistes organites peab iga asjassepuutuv NATO liikmesriik ning NATO tsiviil- ja sõjaline organ kehtestama sisekorra, tagamaks et NS tasemel salastatud teave on kontrollitud ning et selle vastuvõtmine, elukäik ning edastamine on registreeritud.

69. NATO arvelevõtmise kohustusega teabe kontrolldokumendid peavad võimaldama tuvastada kõiki isikuid, kes on omanud juurdepääsu nimetatud teabele, et toetada kahjude hindamist või korraldada juurdlus arvelevõtmise kohustusega teabe salajasuse kahjustamise või kaotsimineku asjus.

KASUTUSEST EEMALDAMINE JA HÄVITAMINE

70. NATO salastatud teabe nõuetekohane haldamine katab kogu selle elutsükli, sealhulgas selle kasutusest eemaldamise ja hävitamisega seotud asjaolud. Elutsükli lõpus hinnatakse teabe säilitamise, arhiveerimise, salastatuse taseme alandamise, salastatuse kustutamise või hävitamise vajadust.

71. Kõik nimetatud tegevused peavad vastama nii julgeolekunõuetele kui ka NATO salastatud teabe haldamise ja arhiveerimise nõuetele kooskõlas NATO teabe säilitamise ja elukäigu põhimõtetega (C-M(2009)0021, *Policy on the Retention and Disposition of NATO Information*) ja seda täiendavate direktiividega.

Hävitamine

72. Paberkandjal NATO salastatud teave, mida ei ole enam ametlikeks eesmärkideks vaja, kaasa arvatud üleliigne või asendatud teave ja jäätmed, hävitatakse nii, et seda ei oleks võimalik taastada. Hävitamise protseduuride, sealhulgas selleks eesmärgiks kasutatavate meetodite ja toodete heakskiitmine on riigi julgeoleku volitatud esindajate / volitatud julgeolekuasutuste (NSA/DSA) või muu pädeva julgeolekuasutuse ning NATO tsiviil- ja sõjaliste organite julgeolekuasutuste (NATO julgeolekubüroo, SHAPE J2, ACT julgeolekubüroo) vastutada. Kehtivad järgmised miinimumnõuded.

(a) Paberipurustaja

(i) Kui NATO arvelevõtmise kohustusega teabe lõplikuks hävitamiseks kasutatakse paberipurustajat, siis purustamisel alles jääva tüki suurus ei tohi olla suurem kui 5 mm^2. NR/NC tasemel salastatud teabe puhul ei tohi purustamisel alles jääva tüki suurus olla suurem kui 10 mm^2. Paberipurustaja peab tekitama ristilõikeid, et teave oleks jäädavalt hävitatud. Paberipurustaja peab olema võimalik manuaalselt kasutada ja see peab olema sellise ehitusega, et toimingu jooksul ei jää masinasse hävitamata materjali.

(ii) Kui paberipurustaja ei vasta eespool toodud i punkti nõuetele, kasutatakse asjakohast edasise hävitamise protsessi, mille käigus juurdepääsuõigusega personal kogub purustatud jäätmed kokku ja hävitab need heakskiidetud meetodil või viisil, mis tagab, et volitamata personal saab salastatud jäätmetele juurdepääsu alles siis, kui neid pole võimalik enam taastada.

(iii) Mis tahes kõrvalekalde eespool i ja ii punktides toodud nõuetest kiidab juhtumipõhiselt heaks riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutus (NSA/DSA) või muu pädev julgeolekuasutus riskide hindamise teel.

(b) Purustusseade
Masin peab olema võimeline peenestama salastatud jäätmed kiudude lagundamise teel. Paberimassi peab lagundama ja kiud lõhkuma, et äratuntavat teavet oleks võimatu taastada. Laadimisavale või muule avausele, kust pääseb juurde paagi sisemusele, tuleb paigaldada lukustusseade, mille saab kinnitada topelt-tabalukkudega.

(c) Põletusahi
Põletusahju ehitus peab olema selline, et sellesse on võimalik paigutada pitseeritud salastatud jäätmete kotte. Mis tahes avaus, mis võimaldab juurdepääsu salastatud

jäätmetele või tuhale põletamise ajal või pärast seda peab olema pitseeritud või tabalukuga suletud. Tuhajääk ei tohi olla äratuntav.

73. Teisaldatava elektroonilise salvestuskandja hävitamisel juhindutakse NATO konsultatsiooni- ja juhtimisnõukogu (C3-nõukogu) juhendist, mis on avaldatud INFOSECI tehnilise rakendamise direktiivina ning süsteemi seadmete ja salvestuskandjate salastatuse taseme alandamise ja hävitamise juhendina (vastavalt AC/322-D(2012)0011, *INFOSEC Technical Implementation Directive* ja AC/322-D(2012)0012, *Guidance on Downgrading and Destruction of System Equipment and Storage Media*).

74. Avaldajalt ei ole vaja oodata hävitamisjuhiseid teabe puhul, mida säilitatakse, aga mis ei ole enam vajalik. Registrid ja muud bürood[6], mille valduses niisugune teave on, vaatavad selle üle ja määravad kindlaks, kas see on endiselt oluline või kas selle võib hävitada.

75. Järgnevalt on toodud lisanõuded arvelevõtmise kohustusega teabe hävitamiseks:

(a) kogu CTS tasemel salastatud teave tagastatakse selle eest vastutavale registrile hävitamiseks. CTS tasemel salastatud teabe kohta koostatakse hävitamise akt, millele kirjutab alla COSMIC juhtiv ametnik (CCO) ja tunnistajana sõltumatu ametnik, kellel on asjakohane juurdepääsuõigus ja volitused CTS tasemel salastatud teabele juurde pääseda;

(b) asjakohase COSMIC põhiregistri COSMIC juhtiv ametnik (CCO) võib volitada mis tahes lähetatud või isoleeritud sõjaväeüksuse vastutavat juhti hävitama CTS tasemel salastatud teavet, mida enam ei vajata, tingimusel et vastutavale registrile antakse nõuetekohaselt vormistatud hävitamise aktid;

(c) CTS tasemel salastatud teabe hävitamise akte ja kontrolldokumente säilitatakse registris vähemalt 10 aastat, kuna neist võib olla abi juurdluseläbiviimisel. Hävitamise aktide koopiaid ei pea edastama avaldajale ega asjakohasele COSMIC põhiregistrile, kui neid selgesõnaliselt ei taotleta;

(d) NS tasemel salastatud teabe hävitamine registreeritakse ning aktile kirjutavad alla hävitamist teostav ametnik ja sõltumatu tunnistaja; mõlemal peab olema asjakohane juurdepääsuõigus ja volitused NS tasemel salastatud teabele juurde pääseda;

(e) NS tasemel salastatud teabe hävitamise akte ja kontrolldokumente säilitatakse registris või teavet hävitavas büroos konkreetse NATO liikmesriigi ning NATO tsiviil- ja sõjalise organi sätestatud tähtaja jooksul, aga mitte vähem kui viis aastat.

76. Kui avaldaja seda ei nõua või kui riiklikes õigusaktides ei ole seda selgesõnaliselt nõutud, ei pea NC ja NR tasemel salastatud teabe hävitamist registreerima ja kontrolldokumente säilitama. Lisateave säilitamise tähtaegade kohta on saadaval NATO teabe säilitamise ja elukäigu põhimõtetes (C-M(2009)0021, *Policy on the Retention and Disposition of NATO Information*) ja seda täiendavates direktiivides.

Turvaintsident

77. Turvaintsident on sündmus või muu juhtum, millel võib olla negatiivne mõju NATO salastatud teabe turvalisusele ja mis vajab täiendavat uurimist, et täpselt määratleda, kas tegu oli turvanõuete rikkumise või väärkäitlusega.

[6] Siia alla kuuluvad allregistrid ja nende isikute bürood, kes on volitatud kõnealust teavet valdama.

Turvanõuete rikkumine

78. Turvanõuete rikkumine on tahtlik või tahtmatu tegevus või tegevusetus, mis on vastuolus NATO julgeolekupoliitikaga (*NATO Security Policy*) ja seda täiendavate direktiividega ning mille tulemusel võib NATO salastatud teabe või tugiteenuste ja ressursside salajasus tegelikult või potentsiaalselt kahjustada saada, sealhulgas:

(a) NATO salastatud teave võib kaotsi minna;

(b) NATO salastatud teabele pääseb juurde personal, kellel pole nõuetekohasel tasemel juurdepääsuluba ja/või teadmisvajadust;

(c) NATO salastatud teavet säilitatakse ebaturvalises kapis või sellises kapis, mida ei ole heaks kiidetud säilitataval tasemel salastatud teabe jaoks;

(d) NATO salastatud teave jäetakse ebaturvalisele alale, kus sellele pääsevad saatjata juurde isikud, kellel ei ole juurdepääsuõigust,

(e) NATO salastatud teavet ei leita selle ootuspärasest asukohast;

(f) NATO salastatud teavet edastatakse viisil, mis pole käesoleva direktiivi alusel lubatud;

(g) NATO salastatud teavet töödeldakse süsteemis, mis ei ole vastava taseme NATO salastatud teabe jaoks nõuetekohaselt akrediteeritud;

(h) NATO salastatud teavet on volitamata muudetud;

(i) NATO salastatud teabele on tahtlikult määratud madalam salastatuse tase;

(j) NATO salastatud teave on hävitatud volitamata viisil või

(k) side- ja infosüsteemis tekib teenusetõkestus.

Salajasuse kahjustamine

79. Salajasuse kahjustamine tähistab olukorda, kus turvanõuete rikkumise või vaenuliku tegevuse tõttu (näiteks spionaaž, terroriaktid, sabotaaž või vargus) ei ole NATO salastatud teave enam salastatud, terviklik või kättesaadav, või tugiteenused või ressursid ei ole enam terviklikud või kättesaadavad. Siia hulka kuulub kaotsiminek, volitamata isikutele avalikustamine (näiteks spionaaži kaudu või meediale), volitamata muutmine, volitamata viisil hävitamine või teenusetõkestus.

80. Sellise NATO salastatud teabe, mis on kasvõi ajutiselt väljapool turvaala kaotsi läinud, salajasus loetakse kahjustatuks. Sellise NATO salastatud teabe, mis on kasvõi ajutiselt kaotsi läinud turvaalal, sealhulgas dokumentide, mida ei suudeta perioodilise inventuuri käigus leida, salajasus loetakse kahjustatuks kuni juurdlusega tõestatakse vastupidist.

Väärkäitlus

81. Väärkäitlus on tahtlik või tahtmatu tegevus või tegevusetus, mis on vastuolus NATO julgeolekupoliitikaga (*NATO Security Policy*) ja seda täiendavate direktiividega ning mille tulemusel ei saa NATO salastatud teabe salajasus tegelikult või potentsiaalselt kahjustada (näiteks NATO salastatud teave jäetakse turvamata turvalises rajatises, kus kõik isikud on asjakohase juurdepääsuõigusega, NATO salastatud teavet ei panda topeltpakendisse jne).

Tegevus turvanõuete rikkumise või väärkäitluse avastamisel

82. Kõigist turvanõuete rikkumistest või võimalikest rikkumistest teavitatakse viivitamatult asjakohast julgeolekuasutust. Iga turvanõuete rikkumist, millest on teavitatud, uurivad julgeoleku, juurdluse ja kui see on asjakohane, siis ka vastuluure kogemusega isikud, kes on sõltumatud isikutest, kes on vahetult turvanõuete rikkumisega seotud, et määrata kindlaks:

(a) kas NATO salastatud teabe salajasus on kahjustatud;

(b) kas kõigil isikutel, kellel oli või võis olla juurdepääs rikkumisega seotud teabele, on vähemalt riiklik juurdepääsuluba või volitused NATO salastatud teabele juurde pääsuks ja kas nad on olemasolevate andmete põhjal niivõrd ausad ja usaldusväärsed, et salajasuse kahjustamisest ei teki NATO-le tõenäoliselt mingit kahju ning

(c) millised kompenseerivad, parandus- või distsiplinaarmeetmed (sealhulgas õiguslikud) on soovituslikud.

83. Kui juurdlus annab jaatavad vastused lõike 82 punktile a kui ka b ja kui on olemas mõistlikud asitõendid, et juurdepääs oli tahtmatu, siis võtab asjakohane julgeolekuasutus meetmeid, et asjassepuutuvatele isikutele kas selgitada või neid koolitada vastava NATO salastatud teabe erikategooria, millele nad tahtmatult juurde pääsesid, reeglitest. Asjakohane julgeolekuasutus võib sellised juhtumid lõpetada ilma NATO julgeolekubürood teavitamata.

84. Kui juurdlus annab eitavad vastused lõike 82 punktile b, siis tuleb salajasuse kahjustamisest teavitada NATO julgeolekubürood, nagu allpool kirjeldatud.

85. Side- ja infosüsteemide julgeoleku põhidirektiivis (AC/35-D/2004, *Primary Directive on CIS Security*) on selgelt sätestatud side- ja infosüsteemidesse puutuvad asjaolud, mille puhul NATO julgeolekubürood tuleb viivitamatult teavitada side- ja infosüsteemide turvaintsidendist, näiteks volitamata suuremahulisest andmete kogumisest.

86. Väärkäitluse puhul võib riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutus (NSA/DSA) selliseid juhtumeid uurida, nendega tegeleda ja need lõpetada ilma NATO julgeolekubürood teavitamata. NATO tsiviil- ja sõjaliste organite asjakohane julgeolekuasutus võib samuti nimetatud juhtumeid uurida, nendega tegeleda ja need lõpetada ilma NATO julgeolekubürood teavitamata, välja arvatud juhul, kui on ilmnenud märke, et juhtum võib korduda või kui on kahtlusi asjassepuutuvate isikute tegevuste või käitumise kohta.

Salajasuse kahjustamisest teavitamine

87. Kui NATO salastatud teabe salajasuse kahjustamisest tuleb lõike 84 alusel teavitada, edastatakse aruanne asjassepuutuva riigi julgeoleku volitatud esindaja / volitatud julgeolekuasutuse (NSA/DSA) või NATO tsiviil- või sõjalise organi juhi kaudu NATO julgeolekubüroole. Kui võimalik, siis peaks aruandev asutus teavitama teabe avaldanud NATO organit samal ajal kui NATO julgeolekubürood, kuid seda võib paluda teha NATO julgeolekubürool, kui avaldajat on keerukas tuvastada. Aruannete ajastus oleneb teabe tundlikkusest ja asjaoludest. Esialgne aruanne edastatakse viivitamatult NATO julgeolekubüroole, kui on kindlaks tehtud, et:

(a) NS, CTS tasemel salastatud või erikategooria tähistega teabe salajasus on kahjustatud;

(b) on märke või kahtlusi, et tegu on spionaažiga (kui aruanne ei takista käsilolevat juurdlust) või

(c) toimunud on volitamata avalikustamine pressile/meediale.

88. Esialgsed aruanded sisaldavad järgnevat teavet:

(a) asjassepuutuva teabe kirjeldus, sealhulgas selle NATO salastatuse tase ja, kui see on teada, siis märgistuse viitenumber ja koopia järjekorranumber, kuupäev, avaldaja, teema ja ulatus;

(b) väga lühike kirjeldus salajasuse kahjustamise asjaoludest, sealhulgas kuupäev; periood, mille jooksul teabe salajasus kahjustada sai ja, kui see on teada, siis nende volitamata isikute arv ja/või kategooria, kellel oli või võis olla juurdepääs ning

(c) asjaolu, kas avaldajat on teavitatud.

89. Täiendavad aruanded esitatakse vastavalt edasistele arengutele. NC tasemel salastatud teabe salajasuse kahjustamise aruanded edastatakse siis, kui juurdlus on lõpetatud ja need peaksid sisaldama lõike 88 punktides a, b ja c nõutud teavet. NR tasemel salastatud teabe salajasuse kahjustamisest ei ole kohustuslik teavitada, välja arvatud kui see vastab lõike 87 punktis b või c sätestatud kriteeriumidele või seda nõutakse selgesõnaliselt riiklikes õigusaktides. Kõikidel salajasuse kahjustamise juhtudel, millest on kohustuslik teavitada, tuleb esitada NATO julgeolekubüroole juurdluse lõpparuanne või vahearuanne 90 päeva jooksul pärast esialgset aruannet.

Turvanõuete rikkumise registreerimine

90. NATO tsiviil- ja sõjaliste organite juhid korraldavad turvanõuete rikkumistega seotud dokumentide, sealhulgas juurdluste ning kompenseerivate ja parandusmeetmete aruannete säilitamise 10 aasta jooksul ning tagavad, et need on julgeolekuinspektsioonide ajal kättesaadavad.

Arvelevõtmise kohustusega dokumentide kaotamise eest jätkuvast vastutusest vabastamine

91. Kui juurdluse lõpparuanne näitab, et arvelevõtmise kohustusega teave on pöördumatult kaotatud, mitte ajutiselt kadunud, ja salajasuse kahjustamine tundub ebatõenäoline, siis võivad riigi julgeoleku volitatud esindajad / volitatud julgeolekuasutused (NSA/DSA) või NATO tsiviil- või sõjalise organi juht asjakohase registri või kontrollpunkti jätkuvast vastutusest vabastada.

Teabe avaldanud NATO tsiviil- või sõjalise organi tegevus

92. NATO salastatud teabe salajasuse kahjustamisest teavitamise peamine eesmärk on võimaldada NATO tsiviil- või sõjalisel organil hinnata NATO-le tekkida võivat kahju ja võtta kasutusele mis tahes meetmeid, mis on vajalikud mõjude vähendamiseks ja juhtumi kordumise vältimiseks. Aruanded kahju hindamise ja vähendamise meetmete kohta edastatakse NATO julgeolekubüroole.

NATO julgeolekubüroo tegevus

93. NATO julgeolekubüroo:

(a) koordineerib juurdlusi, millesse on kaasatud rohkem kui ühe NATO liikmesriigi julgeolekuasutused;

(b) koordineerib vajadusel avaldajate ja asjassepuutuvate julgeolekuasutustega NATO-le tekitatud kahju lõplikku hindamist ja mis tahes meetmeid kahju vähendamiseks;

(c) soovitab korraldada täiendavaid juurdlusi, kui need vajalikuks osutuvad, ja/või korraldab neid kokkuleppel asjassepuutuva julgeolekuasutusega ning

(d) teavitab NATO peasekretäri, kui organisatsioonile tekitatud kahju tõsidus seda nõuab.

NATO peasekretäri tegevus

94. NATO peasekretär võib nõuda, et asjakohased asutused korraldaksid täiendava juurdluse ja esitaksid tulemuste kohta aruande.

KULLERITUNNISTUS

(Näidis)

Kehtib kuni
….....

1. Käesolevaga kinnitatakse, et tunnistuse omanik …..... *(nimi ja auaste, kui on asjakohane)* .....……, passi nr ….....…… omanik, on järgneva organisatsiooni liige *(organisatsiooni nimi)* ……..……..

2. Pöördel üksikasjalikult kirjeldatud marsruudil täidab loa omanik enda ametikohustusi, olles määratud NATO ametlikuks kulleriks. Isik on volitatud transportima ……..... (arv) pakendit ametlike NATO dokumentidega, mille tunnusmärgid vastavad vastava marsruudi kõrval toodud tunnusmärgi näidistele.

3. Kõigil asjassepuutuvatel tolli- ja migratsiooniametnikel palutakse seega tagada tunnistuse omaniku transporditavatele ametliku tunnusmärgiga dokumentidele ja ametlikule kirjavahetusele puutumatus läbiotsimise ja -vaatamise eest Põhja-Atlandi Lepingu Organisatsiooni ning selle liikmesriikide esindajate ja rahvusvahelise personali staatuse kokkuleppe (*Agreement on the Status of the North Atlantic Treaty Organization National Representatives and International Staff*) ja Põhja-Atlandi lepingu osalisriikide vahelise relvajõudude staatust reguleeriva kokkuleppe (*Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces*) alusel. Kui eespool tuvastatud kulleri transporditavate pakendite läbivaatamist peetakse absoluutselt vajalikuks, siis juhitakse tolli- ja migratsiooniametnike tähelepanu järgnevale:
   i. palume, et pakendeid kontrolliksid ainult nõuetekohaselt volitatud isikud või isikud, kellel on vastav luba;
   ii. palume, et pakendeid kontrollitaks avalikkuse pilgu alt väljas oleval alal ja kulleri juuresolekul;
   iii. palume, et kui pakend avatakse kontrollimiseks, siis märgitakse see pärast uuesti sulgemist ära, et tõendada avamist pitseerimise ja allakirjutamisega ning märkega, et pakend avati;
   iv. tolli-, politsei- ja/või migratsiooniametnikel palutakse vajadusel abi pakkuda, et tagada transporditavate dokumentide edukas ja turvaline kätte toimetamine.

Loa väljastanud ametniku allkiri Kuupäev:

Nimi ja ametikoht:
(Nimi ja auaste trükitähtedega)

NATO riigi või NATO tsiviil- või sõjalise organi ametlik pitser

TEEKONNA ANDMED

Saatja Saaja

KASUTATUD TUNNUSMÄRGI NÄIDIS

Vt märkust allpool

MÄRKUS: Lisaks tunnusmärgile peab tunnusmärki lisav ametnik kirjutama trükitähtedes välja oma nime, auastme ja enda osakonna, väejuhatuse, asutuse või rajatise nime ja aadressi.

JUHISED KULLERILE
NATO salastatud teabe käsipostiga transportimiseks

Olete määratud transportima NATO salastatud saadetist. Teile on antud kulleritunnistus. Enne reisi tutvustatakse teile NATO salastatud teabe käsipostiga transportimise turvanõudeid ja teie kohustusi konkreetse reisi jooksul (käitumine, reisiplaan, graafik, jne).

Juhime teie tähelepanu järgmistele üldistele punktidele.

1. Teie vastutate selle saadetise turvalise hoidmise eest, mida teid volitati transportima.

2. Saadetis peab kogu reisi jooksul püsima isiklikult teie valduses ja seda ei tohi mitte mingil juhul jätta järelevalveta.

3. Saadetist ei tohi marsruudil avada, välja arvatud allpool punktis 6 toodud asjaoludel.

4. Hädaolukorras peate saadetise kaitsmiseks võtma kasutamisele enda äranägemisel meetmeid, mida vajalikuks peate, ja ei tohi mitte mingil juhul lubada, et saadetis teie isiklikust valdusest väljub.

5. Teie vastutate selle eest, et teie isiklikud riigist lahkumiseks vajalikud ja reisidokumendid (pass, valuuta ja meditsiinilised dokumendid jne) oleksid täielikud, kehtivad ja ajakohased.

6. OLULINE: Kui tolli-, politsei- ja/või migratsiooniametnikud esitavad küsimusi teie saadetise sisu kohta, näidake neile oma kulleritunnistust ja nõudke, et soovite seda näidata tolli, politsei ja/või migratsiooni kõrgema järgu ametnikule. Sellest tegevusest peaks tavapäraselt piisama, et saadetisega saaks seda avamata edasi minna. Kui aga tolli, politsei ja/või migratsiooni kõrgema järgu ametnik nõuab näha saadetise tegelikku sisu, võite selle tema juuresolekul avada, aga seda peaks tegema avalikkuse pilgu alt väljas olevas piirkonnas.

7. Rakendage ettevaatusabinõusid, et näidata ametnikele sisust üksnes nii palju, et nad veenduksid, et selle hulgas ei ole mingit muud eset ja paluge ametnikul saadetis uuesti ära pakendada või teid pakendamisel abistada kohe kontrolli lõppemisel.

8. Paluge tolli, politsei ja/või migratsiooni kõrgema järgu ametnikul tõendada saadetise avamist ja kontrollimist allakirjutamise ja pitseerimisega, kui see on uuesti suletud, ja kinnitusega saadetise avamise kohta.

9. Marsruudil võite abi palumiseks võtta ühendust järgnevate ametnikega:

(Nimi ja kontaktandmed) .....
.....
(Nimi ja kontaktandmed) .....
.....