Europeiska unionens råd

Bryssel den 20 november 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

LÄGESRAPPORT

från:	Rådets generalsekretariat
av den:	20 november 2017
till:	Delegationerna
Föreg. dok. nr:	13943/17 + COR 1
Komm. dok. nr:	12210/17, 12211/17
Ärende:	Rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet – Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU – Rådets slutsatser (20 november 2017)

För delegationerna bifogas rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet – Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU, som antogs av rådet (allmänna frågor) den 20 november 2017.

BILAGA

Utkast till rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet – Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU

Europeiska unionens råd,

1. SOM INSER cybersäkerhetens betydelse för välståndet, tillväxten och säkerheten i EU och för våra fria och demokratiska samhällens och deras grundläggande processers integritet i den digitala tidsåldern, eftersom den skyddar såväl rättsstatsprincipen som de mänskliga rättigheterna och de grundläggande friheterna,

2. SOM UNDERSTRYKER behovet av att hantera cybersäkerheten med hjälp av en sammanhållen strategi på nationell, europeisk och global nivå, eftersom cyberhoten kan påverka demokratin, välståndet, stabiliteten och säkerheten i våra samhällen,

3. SOM NOTERAR att en hög cyberresiliensnivå i EU också är viktigt för att skapa förtroende för den digitala inre marknaden och vidareutveckla det digitala Europa,

4. SOM UPPREPAR att EU även fortsättningsvis kommer att främja en öppen, global, fri, fredlig och säker cyberrymd, där mänskliga rättigheter och grundläggande friheter, särskilt rätten till yttrandefrihet, tillgång till information, dataskydd, integritet och säkerhet samt EU:s kärnvärderingar och grundläggande principer, tillämpas fullt ut och respekteras både inom EU och globalt, och SOM BETONAR den avgörande betydelsen av att säkerställa en lämplig jämvikt mellan de mänskliga rättigheterna och grundläggande friheterna och kraven i EU:s politik för inre säkerhet[1],

5. SOM INSER att den internationella rätten, bland annat FN-stadgan i sin helhet, den internationella humanitära rätten och människorättslagstiftningen, är tillämplig i cyberrymden, och SOM därmed UNDERSTRYKER behovet av fortsatta insatser i syfte att säkerställa att internationell rätt respekteras i cyberrymden,

[1] Dok. 12650/17.

6. SOM ERINRAR OM sina slutsatser om EU:s strategi för cybersäkerhet[2], om förvaltning av internet[3], om förstärkning av EU:s cyberresiliens[4], om cyberdiplomati[5] och om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet[6], om förbättrad straffrätt i cyberrymden[7], om säkerhet och försvar inom ramen för EU:s globala strategi[8], om den gemensamma ramen för att motverka hybridhot[9] och om halvtidsöversynen av den förnyade strategin för inre säkerhet i Europeiska unionen 2015–2020[10],

7. SOM INSER att den ram som tillhandahålls genom Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen) utgör en solid grund som gör att en heterogen grupp länder kan använda en effektiv rättslig standard för de olika nationella lagstiftningarna och för det internationella samarbetet mot cyberbrott,

8. SOM INSER behovet av att lägga förnyad betoning på genomförandet av ramen för EU:s politik för it-försvar från 2014 och att uppdatera den i syfte att ytterligare integrera cybersäkerhet och cyberförsvar i den gemensamma säkerhets- och försvarspolitiken (GSFP) och i den övergripande agendan för säkerhet och försvar,

9. SOM INSER att en globalt konkurrenskraftig europeisk industri är en viktig faktor för att en hög cybersäkerhetsnivå ska kunna uppnås nationellt och inom hela EU,

10. SOM ERINRAR OM att den nationella säkerheten enligt artikel 4.2 i EU-fördraget är varje medlemsstats eget ansvar,

---

2 Dok. 12109/13 och 6225/13 (Gemensamt meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd* (JOIN(2013) 1 final)).

3 Dok. 16200/14 och 6460/14 (Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *Internetpolitik och förvaltning av internet: Europas roll i utformningen av framtidens internetförvaltning* (COM(2014) 72 final)).

4 Dok. 14540/16 och 11013/16 (Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – *Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch* (COM(2016) 410 final)).

5 Dok. 6122/15.

6 Dok. 9916/17.

7 Dok. 10007/16.

8 Dok. 9178/17.

9 Dok. 7688/16 (Gemensamt meddelande till Europaparlamentet och rådet – *Gemensam ram för att motverka hybridhot: Europeiska unionens insatser*).

10 Dok. 12650/17.

11. VÄLKOMNAR HÄRMED det gemensamma meddelandet till Europaparlamentet och rådet med titeln *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*, och dess ambitiösa mål att öka cybersäkerheten i EU; det bidrar också till att förstärka EU:s strategiska autonomi, i linje med rådets slutsatser om den globala strategin för Europeiska unionens utrikes- och säkerhetspolitik[11], genom målsättningen att bygga ett digitalt Europa som är mer säkert, förtroendeskapande, medvetet om sina starka sidor, konkurrenskraftigt, öppet för omvärlden, respektfullt för EU:s gemensamma värderingar i fråga om ett öppet, fritt, fredligt och säkert internet – och som därmed uppnår en högre resiliensnivå när det gäller att förebygga, avskräcka från, upptäcka och vidta åtgärder mot cyberhot och gemensamt kunna reagera på cyberhot i hela EU,

12. UPPMANAR medlemsstaterna och EU:s institutioner, byråer och organ att samarbeta, med respekt för varandras behörighetsområden och subsidiaritets- och proportionalitetsprinciperna, som svar på de strategiska mål som anges i dessa slutsatser,

13. UNDERSTRYKER behovet av att EU, dess medlemsstater och den privata sektorn säkerställer tillräcklig finansiering, med hänsyn tagen till tillgängliga medel, i syfte att stödja uppbyggnaden av cyberresiliens och cybersäkerhetsrelaterade forsknings- och utvecklingsinsatser i hela EU och att stärka samarbetet för att förebygga, avskräcka från, upptäcka och vidta åtgärder mot cyberhot och gemensamt kunna reagera på storskaliga cyberincidenter och skadlig it-verksamhet i hela EU,

---

[11] Dok. 13202/16.

Kapitel I

SÄKERSTÄLLANDE AV EN EFFEKTIV EU-CYBERRESILIENS OCH TILLTRON TILL DEN DIGITALA INRE MARKNADEN

14. UNDERSTRYKER att medlemsstaterna har huvudansvaret för att stärka sin egen cybersäkerhet och säkerställa sin respons på cyberrelaterade incidenter och kriser samtidigt som EU kan tillföra ett tydligt mervärde genom att främja samarbetet mellan medlemsstaterna; BETONAR i detta sammanhang behovet av att samtliga medlemsstater ställer nödvändiga medel till förfogande för de nationella myndigheter som är ansvariga för cybersäkerheten i syfte att säkerställa förebyggande, upptäckt och bekämpning av cyberrelaterade incidenter och kriser i hela EU,

15. UNDERSTRYKER behovet av att där så är möjligt utnyttja befintliga mekanismer, strukturer och organisationer på EU-nivå,

16. LOVORDAR

- de framsteg som medlemsstaterna gjort när det gäller att införliva it-säkerhetsdirektivet och BETONAR att det måste vara fullständigt och effektivt genomfört senast i maj 2018 i enlighet med det direktivet[12],
- det arbete som utförts inom den samarbetsgrupp som genom it-säkerhetsdirektivet inrättats i syfte att stärka strategiskt samarbete och informationsutbyte mellan medlemsstaterna,
- det arbete som utförts inom CSIRT-nätverket, framför allt i syfte att stärka det operativa samarbetet mellan medlemsstaterna, skapa tilltro och förtroende när det gäller informationsutbyte vid hanteringen av storskaliga cybersäkerhetsincidenter och, baserat på nationella slutsatser från medlemsstater, och att bidra till en gemensam situationsmedvetenhet på europeisk nivå,
- det arbete som utförts inom det avtalsbaserade offentlig-privata partnerskapet för cybersäkerhet,

[12] Utan att det påverkar medlemsstaternas befogenhet med avseende på införlivandet av it-säkerhetsdirektivet, i synnerhet vad gäller leverantörer av samhällsviktiga tjänster.

17. VÄLKOMNAR det gemensamma meddelandets bekräftelse av att en stark och tillförlitlig kryptering är mycket viktigt för att mänskliga rättigheter och grundläggande friheter ska kunna säkerställas i EU och för att allmänheten ska ha tilltro till den digitala inre marknaden, samtidigt som hänsyn tas till de brottsbekämpande myndigheternas behov av att få åtkomst till data som krävs för deras utredningar, samt bekräftelsen av att såväl säker digital identifiering som kommunikation spelar en avgörande roll för att säkerställa effektiv cybersäkerhet i EU,

18. VÄLKOMNAR planen i det gemensamma meddelandet att höja ambitionsnivån när det gäller att regelbundet anordna Europaomfattande cybersäkerhetsövningar på basis av erfarenheter från övningar inom ramen för *Cyber Europe*, med en kombination av insatser på olika nivåer, eftersom detta kommer att utgöra ett viktigt inslag för att främja medlemsstaternas och EU-institutionernas beredskap för att hantera storskaliga cyberincidenter,

19. UPPMANAR EU och dess medlemsstater att regelbundet genomföra strategiska cybersäkerhetsövningar i olika rådskonstellationer på basis av de erfarenheter som inhämtades under EU Cybrid 2017 och

20. – utan att det påverkar resultatet av lagstiftningsprocessen –

- VÄLKOMNAR förslaget om ett starkt och permanent mandat för Enisa med primärt mål att stödja och utveckla ett närmare samarbete mellan medlemsstaterna, öka deras kapacitet och öka förtroendet för ett digitalt Europa,

- BEKRÄFTAR att det framtida Enisa bör bygga på erfarenheterna och sakkunskapen i medlemsstaterna och EU samt stödja konsekvent utveckling och genomförande av befintlig och kommande EU-politik och EU-bestämmelser för cybersäkerhet, samtidigt som det säkerställs att alla Enisas befogenheter utvecklas för att komplettera medlemsstaternas,

- BEKRÄFTAR målet om stärkt förtroende för det digitala Europa genom ökad tilltro till och ökat förtroende för digitala lösningar och innovationer, inbegripet sakernas internet, e-handeln och e-förvaltning, särskilt när det gäller en europeisk ram i världsklass för cybersäkerhetscertifiering[13]; detta är en viktig förutsättning för att tilltron till och säkerheten för digitala produkter och tjänster ska kunna stärkas och kritisk infrastruktur samt förvaltningarnas, medborgarnas och företagens data skyddas, och det medverkar i hög grad till att införa en *security by design*-metod för produkter, tjänster och processer på den digitala inre marknaden,

- BETONAR att lagstiftningsarbetet för stärkt cybersäkerhetcertifiering på EU-nivå måste tillgodose marknadens och användarnas behov, bygga vidare på erfarenheterna av certifieringskapacitet och certifieringsprocesser inom EU (t.ex. inom ramen för gruppen av höga tjänstemän på informationssäkerhetsområdet) och tillhandahålla en ram som snabbt kan anpassas till den framtida digitala utvecklingens tekniska nivå,

- BETONAR att hela spektrumet av säkerhetskrav bör omfattas i arbetet med att förbättra cybersäkerhetcertifieringen i EU, upp till de högsta nivåerna, där motståndskraften mot angripares kapacitet måste bevisas; de viktigaste framgångsfaktorerna skulle vara att säkerställa ett tillförlitligt, öppet och oberoende förfarande för säkerhetscertifiering i syfte att främja tillgången till tillförlitlig och säker utrustning och programvara samt tillförlitliga och säkra tjänster på och utanför den inre marknaden, att erkänna den europeiska industrins och de europeiska regeringarnas och utvärderingsspecialisternas respektive sakkunskap genom europeiska och globala standarder[14], samt att respektera medlemsstaternas roll i certifieringsprocessen, i synnerhet när det gäller utvärdering på högre skyddsnivåer och särskilt i relation till bedömning av väsentliga säkerhetsbehov och säkerhetskompetenser; sådan certifiering bör dessutom säkerställa att varje EU-omfattande certifieringssystem står i proportion till den säkerhetsnivå som krävs för användningen av berörda IKT-relaterade produkter, tjänster och/eller system, och att det möjliggör gränsöverskridande handel för företag av alla storlekar i syfte att utveckla och sälja nya produkter, både inom EU och utanför EU,

---

13 Genom globala standarder som utvecklas i enlighet med reglerna för god praxis i WTO:s avtal om tekniska handelshinder.

14 Genom europeiska och globala standarder som utvecklas i enlighet med reglerna för god praxis i WTO:s avtal om tekniska handelshinder.

21. VÄLKOMNAR avsikten att inrätta ett nätverk av kompetenscentrum för cybersäkerhet för att stimulera utvecklingen och införandet av cybersäkerhetsteknik och ytterligare driva på EU-industrins innovation på den globala arenan när det gäller utvecklingen av nästa generations banbrytande teknik, såsom artificiell intelligens, kvantdatorteknik, blockkedjeteknik och säkra digitala identiteter,

22. BETONAR att nätverket av kompetenscentrum för cybersäkerhet måste vara inkluderande gentemot alla medlemsstater och deras befintliga expertcentrum och kompetenscentrum samt fästa särskild vikt vid komplementaritet, och NOTERAR med detta i åtanke det planerade europeiska cybersäkerhets- och forskningscentrumet, som främst bör fokusera på att säkerställa komplementaritet och undvika dubbelarbete inom nätverket av kompetenscentrum för cybersäkerhet och med andra EU-byråer,

23. BETONAR att nätverket av kompetenscentrum för cybersäkerhet bör hantera en mängd olika ämnesområden, från forskning till industri, och att det därför bland annat bör bidra till att nå målet om en europeisk strategisk autonomi,

24. BEKRÄFTAR i fråga om det föreslagna nätverket av kompetenscentrum för cybersäkerhet att EU, via sina medlemsstater, behöver utveckla en europeisk kapacitet för att utvärdera den kryptografiska styrkan hos produkter och tjänster som är tillgängliga för medborgare, företag och förvaltningar inom den digitala inre marknaden och är samtidigt medvetet om att kryptografipolitik är en nyckelaspekt av nationell säkerhet och därmed är medlemsstaternas befogenhet,

25. UPPMANAR alla relevanta intressenter att öka investeringarna i cybersäkerhetstillämpningar av ny teknik i syfte att bidra till att säkerställa cybersäkerhet i alla sektorer inom den europeiska ekonomin,

26. BETONAR vikten av ett trovärdigt, tillförlitligt och samordnat tillhandahållande av cybersäkerhetstjänster till EU-institutionerna och UPPMANAR KOMMISSIONEN och övriga EU-institutioner att vidareutveckla Cert-EU i enlighet med dessa syften och att säkerställa tillräckliga resurser även för detta,

27. VÄLKOMNAR uppmaningen om att erkänna utomstående säkerhetsforskares viktiga roll för att upptäcka sårbarheter i befintliga produkter och tjänster och UPPMANAR medlemsstaterna att utbyta bästa praxis för att samordna informationen om sårbarheter,

28. BETONAR allas ansvar för cybersäkerheten och UPPMANAR EU och dess medlemsstater att främja digitala färdigheter och mediekompetens för att hjälpa användarna att skydda sin digitala information online och öka deras kunskaper om riskerna med att lägga ut personuppgifter på internet,

29. VÄLKOMNAR att tonvikten i det gemensamma meddelandet läggs vid utbildning, säkert beteende på nätet och medvetenhet i medlemsstaterna och EU,

30. UPPMANAR KOMMISSIONEN att inom kort tillhandahålla en konsekvensbedömning av och senast i mitten av 2018 föreslå de relevanta rättsliga instrumenten för genomförandet av initiativet om inrättade av ett nätverk av kompetenscentrum för cybersäkerhet och ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet,

31. UPPMANAR medlemsstaterna

- att prioritera cybermedvetenhet i informationskampanjer och uppmuntra införandet av cybersäkerhet i akademiska program, utbildningsprogram och yrkesutbildning; man bör särskilt fokusera på utbildning av ungdomar och främjande av deras digitala färdigheter i syfte att förbereda framtidens yrkespersoner på utmaningarna inom säkerhet, ekonomi och tjänster,

- att påskynda inrättandet av specialiserade cybersäkerhetsprogram på hög nivå i syfte att komma till rätta med den aktuella bristen på cybersäkerhetsexperter i EU,

- att inrätta ett effektivt nätverk för samarbete mellan kontaktpunkter för utbildning under Enisas överinseende; nätverket av kontaktpunkter bör sikta på att förbättra medlemsstaternas samordning och utbyte av bästa praxis om utbildning och medvetenhet, samt kurser, övningar och kapacitetsuppbyggnad, på området för cybersäkerhet

- att överväga att tillämpa it-säkerhetsdirektivets bestämmelser även på offentliga förvaltningar som medverkar i kritisk samhällelig och ekonomisk verksamhet, om sådan verksamhet inte redan omfattas av nationell lagstiftning och om det anses lämpligt, samt att tillhandahålla cybersäkerhetskurser även i offentliga förvaltningar med tanke på dessas roll i samhället och ekonomin,

Kapitel II

UPPBYGGNAD AV EU-KAPACITET FÖR ATT FÖREBYGGA, AVSKRÄCKA FRÅN, UPPTÄCKA OCH VIDTA ÅTGÄRDER MOT SKADLIG IT-VERKSAMHET

32. BETONAR att en särskilt allvarlig cyberincident eller cyberkris skulle kunna vara en tillräcklig grund för en medlemsstat att åberopa EU:s solidaritetsklausul[15] och/eller klausulen om ömsesidigt bistånd[16],

33. VÄLKOMNAR antagandet av en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet som bidrar till konfliktförebyggande, samarbete och stabilitet i cyberrymden genom att det där fastställs åtgärder inom ramen för Gusp, däribland restriktiva åtgärder, som kan användas för att förebygga och reagera på skadliga cyberaktiviteter och UPPMANAR utrikestjänsten och medlemsstaterna att regelbundet genomföra övningar inom denna ram,

---

15 Artikel 222 i EUF-fördraget.
16 Artikel 42.7 i EU-fördraget.

34. BETONAR att det behövs en effektiv respons på EU-nivå på storskaliga cyberincidenter och cyberkriser, med respekt för medlemsstaternas befogenheter, och att cybersäkerhet behöver integreras i befintliga krishanteringsmekanismer på EU-nivå[17]; EFTERLYSER därför regelbundna övningar om responsen på EU-nivå på storskaliga cyberincidenter – från diplomatisk-strategisk till teknisk respons – baserat på relevanta ramar och förfaranden, som vid behov kan förbättras[18],

35. BETONAR vikten av välintegrerade mekanismer för respons och informationsutbyte mellan olika aktörer som är av avgörande betydelse för att säkerställa cybersäkerheten i Europa, inbegripet mellan relevanta EU-organ och medlemsstaternas myndigheter; sådana mekanismer kommer att behöva testas och verifieras som en del av cybersäkerhetsövningarna på EU-nivå och vid behov formaliseras genom avtal,

36. NOTERAR möjligheten att undersöka, ifall kommissionen lägger fram ett förslag om inrättande av en fond för hantering av cybersäkerhetsincidenter parallellt med medlemsstaternas befintliga insatser och med respekt för tillgängliga resurser (särskilt inom EU:s fleråriga budgetram), eventuell hjälp till medlemsstaterna att reagera på och begränsa storskaliga cyberincidenter, förutsatt att de har infört ett lämpligt cybersäkerhetssystem före incidenten och fullständigt har genomfört it-säkerhetsdirektivet samt har väletablerade riskhanterings- och övervakningssystem på nationell nivå,

37. ÄR MEDVETET OM de tilltagande kopplingarna mellan cybersäkerhet och försvar och UPPMANAR till ett intensifierat samarbete om cyberförsvar, inbegripet genom att främja samarbete mellan civila och militära incidenthanteringsaktörer och att fortsätta stärka cybersäkerheten för GSFP-uppdrag och GSFP-insatser,

---

17 Dok. C/2017/6100 final.
18 Dok. 9916/17 och C/2017/6100 final.

38. BETONAR behovet av att om möjligt dra full nytta av de föreslagna försvarsinitiativen för att påskynda utvecklingen av adekvat cyberkapacitet i Europa och INSER möjligheterna med att om möjligt utarbeta cyberförsvarsprojekt inom ramen för ett permanent strukturerat samarbete, om deltagande medlemsstater anser att detta är nödvändigt, och ÄR MEDVETET OM den uppgift som den europeiska försvarstekniska och försvarsindustriella basen samt den bredare civila industribasen inom cybersäkerhet har vad gäller att förse medlemsstaterna med verktyg för att skydda sin cyberrelaterade säkerhet och sina försvarsintressen,

39. NOTERAR kommissionens förslag om att införa en utbildningsplattform för cyberförsvar i slutet av 2018 och BETONAR att denna plattform bör öka utbildningsmöjligheterna inom medlemsstaterna och bör komplettera andra EU-insatser och EU-initiativ, i synnerhet Esfa and EDA,

40. UPPMANAR EU och dess medlemsstater att vara handlingskraftiga i fråga om hot i form av IKT-stödd stöld av immateriell egendom, inbegripet företagshemligheter eller annan konfidentiell affärsinformation, i avsikt att ge konkurrensfördelar till företag eller kommersiella sektorer,

41. ÄR MEDVETET OM behovet av att hantera it-brottslighet, inbegripet på dark web, sexuell exploatering av barn online samt bedrägeri och förfalskning av andra betalningsmedel än kontanter, i synnerhet genom att man eftersträvar en bättre kriminalunderrättelsebild, gör gemensamma utredningar och samarbetar om operativt stöd,

42. VÄLKOMNAR EU:s och medlemsstaternas arbete med att hantera de utmaningar som utgörs av system som gör det möjligt för brottslingar och terrorister att kommunicera via vägar som behöriga myndigheter inte har tillgång till; BETONAR att detta arbete måste utföras med beaktande av att stark och tillförlitlig kryptering är av stor vikt för cybersäkerheten och för tilltron till den digitala inre marknaden och respekten för mänskliga rättigheter och grundläggande friheter,

43. UNDERSTRYKER vikten av att ge brottsbekämpande myndigheter verktyg som gör det möjligt att upptäcka, utreda och lagföra it-brottslighet, så att brott som begås i cyberrymden inte blir oupptäckta eller ostraffade och VÄLKOMNAR bidraget från det europeiska rättsliga nätverket mot it-brottslighet i kampen mot brottslighet genom samarbete mellan rättsliga myndigheter,

44. BETONAR vikten av att säkerställa en samordnad EU-ståndpunkt för att på ett effektivt sätt utforma de europeiska och globala internetförvaltningsbesluten inom flerpartsgemenskapen, exempelvis att säkerställa snabbtillgängliga och tillförlitliga Whois-databaser med IP-adresser och domännamn, så att brottsbekämpningskapacitet och allmänna intressen skyddas,

45. BETONAR vikten av att tillämpa internetprotokollet IPv6, som är avgörande för att sakernas internet ska kunna utvecklas i stor skala samt för att förbättra uppklarandet av it-brottslighet,

46. STÖDER det pågående arbetet med gränsöverskridande tillgång till elektroniskt bevismaterial, hantering av datalagring och de utmaningar för straffrättsliga förfaranden som utgörs av system där brottslingar och terrorister kan kommunicera via vägar som behöriga myndigheter inte har tillgång till, med beaktande av att de mänskliga rättigheterna, de grundläggande friheterna och dataskyddet måste respekteras,

47. UPPMANAR kommissionen

- att senast i december 2017 lägga fram en lägesrapport om genomförandet av praktiska åtgärder för att förbättra den gränsöverskridande tillgången till elektroniskt bevismaterial,
- att i början av 2018 lägga fram ett lagstiftningsförslag för att förbättra den gränsöverskridande tillgången till elektroniskt bevismaterial,

48. UPPMANAR Europol, Enisa och Eurojust

- att fortsätta att stärka sitt samarbete i kampen mot it-brottslighet, både med varandra och med andra relevanta aktörer, inklusive CSIRT-nätverket, Interpol, den privata sektorn och den akademiska världen, och därmed säkerställa synergieffekter och komplementaritet, i enlighet med sina respektive mandat och befogenheter,

- att tillsammans med medlemsstaterna bidra till en samordnad strategi för EU:s brottsbekämpande insatser mot storskaliga cyberincidenter och cyberkriser som kompletterar de förfaranden som anges i de relevanta ramarna[19],

49. UPPMANAR EU och dess medlemsstater att fortsätta arbetet med att

- undanröja hinder för brottsutredningar och för en effektiv straffrätt i cyberrymden samt att stärka det internationella samarbetet och den internationella samordningen i kampen mot it-brottslighet,

- hantera de utmaningar som anonymiseringstekniken innebär och samtidigt ta hänsyn till att en stark och tillförlitlig kryptering är av stor vikt för cybersäkerheten och tilltron till den digitala inre marknaden,

- utforma internetförvaltningsbeslut som påverkar de brottsbekämpande myndigheternas kapacitet att bekämpa it-brottslighet,

[19] Dok. 9916/17 och C/2017/6100 final.

Kapitel III

STÄRKANDE AV DET INTERNATIONELLA SAMARBETET FÖR EN ÖPPEN, FRI, FREDLIG OCH SÄKER GLOBAL CYBERRYMD

50. INSER att säkerställandet av cybersäkerhet är en global utmaning som kräver ett effektivt internationellt samarbete mellan alla aktörer, och INSER att en särskild tonvikt måste läggas vid att upprätthålla demokratiska värden och principerna om en öppen, fri, fredlig och säker global cyberrymd, och

51. UPPMANAR med detta i åtanke EU och dess medlemsstater att främja inrättandet av en strategisk ram för konfliktförebyggande, samarbete och stabilitet i cyberrymden med utgångspunkt i tillämpningen av befintlig internationell rätt, särskilt FN-stadgan i sin helhet, utvecklingen och genomförandet av universella normer för staters ansvarsfulla agerande samt regionala förtroendeskapande åtgärder mellan stater,

52. ÄR MEDVETET OM Förenta nationernas roll i vidareutvecklingen av normer för staters ansvarsfulla agerande i cyberrymden och erinrar om att resultaten av diskussionerna i FN:s grupp av regeringsexperter under åren har utmynnat i en överenskommen uppsättning normer och rekommendationer[20] som generalförsamlingen vid ett flertal tillfällen har ställt sig bakom, och som stater bör använda som en grund för ett ansvarsfullt agerande i cyberrymden,

53. ÄR MEDVETET OM att dessa normer för staters ansvarsfulla agerande bland annat innebär att stater inte medvetet bör tillåta att deras territorium används för internationellt olagliga handlingar, att de bör svara på lämpliga framställningar om bistånd från en annan stat vars kritiska infrastruktur är föremål för skadlig IKT-verksamhet som härrör från deras territorium, och att stater bör vidta lämpliga åtgärder för att skydda sin kritiska infrastruktur mot IKT-hot,

54. ÄR MEDVETET OM de gemensamma cyberhot och cyberrisker som EU, Nato och deras respektive medlemsstater står inför och UPPREPAR vikten av fortsatt samarbete mellan EU och Nato om cybersäkerhet och försvar, med full respekt för EU:s principer om delaktighet, ömsesidighet och beslutsautonomi och i enlighet med slutsatserna av den 6 december 2016 om genomförandet av den gemensamma förklaringen från Europeiska rådets ordförande, Europeiska kommissionens ordförande och Natos generalsekreterare[20],

55. UPPMANAR EU och dess medlemsstater att stödja och främja utvecklingen av regionala förtroendeskapande åtgärder, som är en viktig faktor för att öka samarbetet och öppenheten och minska risken för konflikter; genomförandet av förtroendeskapande åtgärder för cybersäkerhet inom ramen för OSSE och andra regionala sammanhang kommer att öka förutsägbarheten i fråga om staters agerande och ytterligare bidra till att stabilisera cyberrymden;

56. BEKRÄFTAR att EU kommer att fortsätta att upprätthålla sina kärnvärderingar genom att skydda de mänskliga rättigheterna och de grundläggande friheterna med utgångspunkt i EU:s riktlinjer för mänskliga rättigheter online; EU betonar även vikten av att alla aktörer, däribland den akademiska världen, det civila samhället och den privata sektorn, medverkar i förvaltningen av internet;

57. UPPMANAR EU och dess medlemsstater att främja uppbyggnad av cyberkapacitet i tredjeländer, och då särskilt prioritera EU:s grannskap och utvecklingsländer där internetanslutningen ökar i snabb takt, i kampen mot it-brottslighet och uppbyggnaden av cyberresiliens, i enlighet med EU:s kärnvärderingar; för att påskynda EU:s insatser på detta område bör ett EU-nätverk för kapacitetsuppbyggnad på cyberområdet och EU-riktlinjer för kapacitetsuppbyggnad på cyberområdet utarbetas, och dessa bör komplettera befintliga mekanismer och strukturer;

---

[20] Dok. 15283/16.

58. UNDERSTRYKER de framsteg som gjorts i samarbetet mellan EU och Nato i fråga om cyberförsvar och cybersäkerhet och utvecklingen i fråga om utbildning och koncept, samtidigt som man undviker onödigt dubbelarbete där kraven överlappar varandra och främjar interoperabilitet med hjälp av krav och standarder för cyberförsvar och UPPMANAR till fortsatt samarbete om cyberförsvarsövningar (för personal) och utbyte av god praxis vad gäller krishantering, samtidigt som man undviker onödigt dubbelarbete där kraven överlappar varandra, med full respekt för EU:s övningspolicy och EU:s principer om delaktighet, ömsesidighet och beslutsautonomi,

59. ÄR MEDVETET OM att Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen) är en effektiv rättslig standard som ska utgöra underlag till nationell lagstiftning om it-brottslighet, UPPMANAR alla länder att utforma lämpliga nationella rättsliga ramar och samarbeta inom den befintliga internationella ram som Budapestkonventionen utgör,

60. ERINRAR OM det som har uppnåtts genom EU:s bilaterala cyberdialoger och efterlyser ytterligare insatser för att underlätta samarbetet med tredjeländer när det gäller cybersäkerhet,

61. ERINRAR OM att EU har en robust och rättsligt bindande exportkontrollmekanism som bygger på de beslut och den bästa praxis som utarbetats inom internationella icke-spridningssystem och NOTERAR den pågående diskussionen i rådet för att finna de bästa sätten att ytterligare förbättra kontrollernas funktion och UPPMANAR medlemsstaterna att fortsätta att i de relevanta internationella exportkontrollsystemen (exempelvis Wassenaar-arrangemanget) hantera de kritiska cybersäkerhetstillämpningarna av ny teknik för att säkerställa en effektiv kontroll av morgondagens kritiska cybersäkerhetsteknik.

62. Som en uppföljning av Europeiska rådets slutsatser av den 19 oktober 2017[21] kommer dessa slutsatser att genomföras med hjälp av en handlingsplan som rådet ska anta före utgången av 2017. Handlingsplanen blir ett levande dokument som rådet regelbundet kommer att se över och uppdatera.

---

[21] Dok. EUCO 14/17.