Rådet for
Den Europæiske Union

Bruxelles, den 19. november 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RESULTAT AF DRØFTELSERNE

fra:	Generalsekretariatet for Rådet
dato:	19. november 2018
til:	delegationerne
Vedr.:	Ramme for EU's cyberforsvarspolitik (2018-ajourføring)

Vedlagt følger til delegationerne ramme for EU's cyberforsvarspolitik (2018-ajourføring), der blev vedtaget af Rådet på 3652. samling den 19. november 2018.

BILAG

RAMME FOR EU'S CYBERFORSVARSPOLITIK

(SOM AJOURFØRT I 2018)

Anvendelsesområde og mål

For at kunne reagere på skiftende sikkerhedsudfordringer er EU og dets medlemsstater nødt til at styrke cyberrobustheden og udvikle solide cybersikkerheds- og cyberforsvarskapaciteter.

Rammen for EU's cyberforsvarspolitik støtter udvikling af EU-medlemsstaternes cyberforsvarskapaciteter samt styrkelse af cyberbeskyttelsen af EU's sikkerheds- og forsvarsinfrastruktur, uden at dette berører medlemsstaternes nationale lovgivning eller EU-lovgivningen, herunder, når det er defineret, anvendelsesområdet for cyberforsvar.

Cyberspace er det femte operationsområde sammen med land-, sø-, luft- og rumområdet: Vellykket gennemførelse af EU-missioner og -operationer er i stigende grad afhængig af uafbrudt adgang til et sikkert cyberspace og kræver derfor solide og robuste operationelle cyberkapaciteter.

Formålet med den ajourførte ramme for EU's cyberforsvarspolitik er at videreudvikle EU's cyberforsvarspolitik ved at tage højde for relevant udvikling inden for andre relevante fora og politikområder og gennemførelsen af rammen siden 2014. Rammen for EU's cyberforsvarspolitik peger på prioriterede områder for cyberforsvar og præciserer rollerne for de forskellige europæiske aktører, samtidig med at den fuldt ud respekterer EU-aktørernes og medlemsstaternes ansvarsområder og kompetencer samt EU's institutionelle ramme og dets selvstændige beslutningstagning.

Baggrund

Det Europæiske Råds konklusioner om FSFP fra december 2013 og Rådets konklusioner om FSFP fra november 2013 opfordrer til udvikling af en ramme for EU's cyberforsvarspolitik på grundlag af et forslag fra den højtstående repræsentant i samarbejde med Europa-Kommissionen og Det Europæiske Forsvarsagentur (EDA). Rammen for EU's cyberforsvarspolitik blev vedtaget af Rådet den 18. november 2014[1], og siden da har konkrete resultater via gennemførelsen heraf bidraget til at styrke medlemsstaternes cyberforsvarskapaciteter i betydelig grad. Som led i årsrapporten 2017 om gennemførelse af rammen for cyberforsvarspolitikken[2] og under hensyntagen til EU's initiativer på sikkerheds- og forsvarsområdet, navnlig den samordnede årlige gennemgang vedrørende forsvar (CARD), det permanente strukturerede samarbejde (PESCO), Den Europæiske Forsvarsfond og den civile FSFP-aftale samt 2018-revisionen af kapacitetsudviklingsplanen (CDP) og planen for udvikling af civil kapacitet, har medlemsstaterne opfordret til en ajourføring af rammen for EU's cyberforsvarspolitik.

Cybersikkerhed er en prioritet i den globale strategi for EU's udenrigs- og sikkerhedspolitik og inden for EU's ambitionsniveau[3]. Den globale strategi fremhæver behovet for at øge kapaciteterne til at beskytte EU og dets borgere og reagere på eksterne kriser. Strategien understreger, at det er nødvendigt at styrke EU som et sikkerhedsfællesskab. I denne forbindelse bør sikkerheds- og forsvarsbestræbelserne også styrke EU's strategiske rolle og dets evne til at handle selvstændigt, når og hvis det er nødvendigt, og med partnere overalt, hvor det er muligt. Disse mål kræver mere samarbejde om kapacitetsudvikling, hvilket vil fremme effektiviteten og interoperabiliteten af de resulterende civile og militære kapaciteter.

---

1 Rådets dokument 15585/14 af 18.11.2014.
2 Rådets dokument 15870/17 af 19.12.2017.
3 Rådets konklusioner af 14. november 2016 om gennemførelse af EU's globale strategi på sikkerheds- og forsvarsområdet.

Det fælles sæt forslag til gennemførelse af den fælles erklæring, som formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for Den Nordatlantiske Traktats Organisation undertegnede den 8. juli 2016 i Warszawa[4], omfatter konkrete tiltag til at udvide EU's og NATO's samarbejde om cybersikkerhed og -forsvar, blandt andet inden for rammerne af missioner og operationer samt vedrørende udvikling af cyberforsvarskapacitet, forskning og teknologi, uddannelse, øvelser og integration af cybersikkerhed i krisestyring. Dette samarbejde finder sted under fuld overholdelse af principperne om åbenhed, gennemsigtighed, inklusivitet, gensidighed og EU's beslutningsautonomi. En teknisk aftale mellem EU's IT-Beredskabsenhed (CERT-EU) og NATO Computer Incident Response Capability (NCIRC), som blev underskrevet i februar 2016, letter teknisk informationsudveksling med henblik på at forbedre forebyggelsen og detekteringen af og reaktionen på cyberhændelser i de to organisationer.

Det bør erindres, at flere EU-politikker bidrager til målene for cyberforsvarspolitikken som beskrevet i dette dokument, og denne ramme tager også hensyn til relevant regulerings-, politik- og teknologistøtte på det civile område. For eksempel vedtog Europa-Parlamentet og Rådet i juli 2016 direktivet om net- og informationssikkerhed[5] (NIS-direktivet), som vil øge medlemsstaternes samlede beredskab over for cybertrusler og styrke samarbejdet i EU. Direktivet fastsætter foranstaltninger med henblik på at opnå et højt fælles sikkerhedsniveau for net- og informationssystemer i Unionen for at forbedre det indre markeds funktion. Fristen for gennemførelse af direktivet var den 9. maj 2018.

---

4 Rådets konklusioner om gennemførelsen af den fælles erklæring fra formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for Den Nordatlantiske Traktats Organisation (af 6. december 2016, dok. 15283/16, og af 5. december 2017, dok. 14802/17). SN 14802/17

5 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

Forslaget fra september 2017 til en EU-forordning om cybersikkerhed omfatter et nyt mandat til EU's Agentur for Cybersikkerhed (ENISA) og oprettelse af en EU-dækkende certificeringsramme. Når certificeringsrammen er oprettet, bør den understøtte høje standarder for IKT-processer, -produkter og -tjenester, være en kilde til konkurrencefordele og øge forbrugeres og indkøberes tillid. Kommissionen tog desuden i september 2017 endnu et skridt til at forberede EU på væsentlige grænseoverskridende cybersikkerhedshændelser (en plan) og arbejder nu sammen med medlemsstaterne og andre institutioner, agenturer og organer om udvikling af et europæisk cybersikkerhedskrisesamarbejde ved at indføre praktisk operationalisering og dokumentation af alle de relevante aktører, processer og procedurer inden for rammerne af EU's eksisterende mekanismer for krisestyring og katastrofehåndtering, navnlig de integrerede ordninger for politisk kriserespons.

Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb fra november 2016 skitserer det fælles mål om at bidrage til EU's strategiske uafhængighed som omhandlet i Rådets konklusioner fra november 2016 om den globale strategi for Den Europæiske Unions udenrigs- og sikkerhedspolitik, herunder i cyberspace. Det Europæiske Råd bekræftede dette budskab i juni 2018 og fremhævede også behovet for at styrke kapaciteter mod cybersikkerhedstrusler fra områder uden for EU.

Rådet vedtog i 2017 en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[6]. Rammen forventes at fremme samarbejde, lette afværgelse af trusler og påvirke adfærden hos potentielle udøvere af ondsindede cyberaktiviteter på lang sigt. Rammen gør brug af FUSP-foranstaltninger, herunder restriktive foranstaltninger, til at forebygge og reagere på ondsindede cyberaktiviteter. Aktører, der står bag ondsindede cyberaktiviteter, skal drages til ansvar for deres handlinger, og EU-medlemsstaterne tilskyndes til at videreudvikle deres evne til at reagere på ondsindede cyberaktiviteter på en koordineret måde i overensstemmelse med den cyberdiplomatiske værktøjskasse. Stater bør ikke udføre eller bevidst støtte informations- og kommunikationsteknologiaktiviteter, der er i strid med deres forpligtelser i henhold til international ret, og bør ikke bevidst tillade, at deres område anvendes til internationale retsstridige handlinger ved hjælp af informations- og kommunikationsteknologi.

Kommissionen og HR/NF forelagde i september 2017 en fælles meddelelse[7] om cybersikkerhed for at begrænse risici som følge af det nye trusselsbillede. Den omfatter cyberforsvar som et af de vigtigste indsatsområder, og rammen for EU's cyberforsvarspolitik er en af grundpillerne i dens konkrete gennemførelse[8].

Rådets konklusioner fra november 2017 om cyberspørgsmål anerkender de voksende forbindelser mellem cybersikkerhed og -forsvar og opfordrer til at intensivere samarbejdet om cyberforsvar, herunder ved at tilskynde til samarbejde mellem civile og militære hændelsesreaktionsgrupper. De påpeger også, at en særlig alvorlig cyberhændelse eller -krise kan være en tilstrækkelig grund for en medlemsstat til at påberåbe sig EU's solidaritetsbestemmelse og/eller bestemmelse om gensidig bistand.

---

6 Rådets konklusioner af 7. juni 2017 om en ramme for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse"), dok. 9916/17.

7 Fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU (af 13. september 2017 – JOIN(2017) 450 final).

8 Rådets konklusioner af 20. november 2017 om den fælles meddelelse til Europa-Parlamentet og Rådet: Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU (dok. 14435/17).

Det permanente strukturerede samarbejde (PESCO) blev iværksat den 11. december 2017. Denne ambitiøse, bindende og inklusive samarbejdsramme er etableret mellem 25 medlemsstater og omfatter et tilsagn om at øge indsatsen inden for samarbejdet om cyberforsvar samt relaterede PESCO-projekter. Første sæt PESCO-projekter, som de deltagende PESCO-medlemsstater udpegede i 2017, omfatter to projekter vedrørende cyberforsvar: "Cyberberedskabshold og gensidig bistand inden for cybersikkerhed" og "Platform til informationsudveksling om reaktion på cybertrusler og -hændelser". Yderligere sæt PESCO-projekter forventes. PESCO vil udvikle cyberforsvarskapaciteter og derfor styrke samarbejdet mellem de deltagende medlemsstater og øge interoperabiliteten.

Den ajourførte EU-kapacitetsudviklingsplan (CDP), som EDA's Styringskomité godkendte i juni 2018, fastlægger cyberforsvar som et nøgleelement og anerkender behovet for defensive cyberoperationer i enhver operationel kontekst på grundlag af avanceret aktuel og forudsigende cyberspacesituationsbevidsthed, herunder evne til at kombinere store mængder data og efterretninger fra mange kilder til støtte for en hurtig beslutningstagning og øget automatisering af dataindsamlings-, analyse- og beslutningsstøtteprocessen. CDP 2018 fastlægger cyberforsvarskapacitetsprioriteter på følgende områder: samarbejde og synergier med relevante aktører på cyberforsvars- og cybersikkerhedsområdet, forsknings- og teknologiaktiviteter vedrørende cyberforsvar, systemudviklingsrammer for cyberoperationer, uddannelse, træning, øvelser og evaluering (ETEE) samt håndtering af cyberforsvarsudfordringer i luften, i rummet, til søs og til lands.

Endelig er det internationale samfunds behov for at forebygge konflikter, samarbejde og stabilisere cyberspace i løbet af de sidste par år blevet klart. EU fremmer i tæt samarbejde med andre internationale organisationer, navnlig FN, OSCE og ASEAN Regional Forum, en strategisk ramme for konfliktforebyggelse, samarbejde og stabilitet i cyberspace, som omfatter i) anvendelse af international ret, særlig FN-pagten i sin helhed, i cyberspace, ii) overholdelse af universelle ikkebindende normer, regler og principper for ansvarlig statslig adfærd og iii) udvikling og gennemførelse af regionale tillidsskabende foranstaltninger (CBM'er). Rammen for cyberforsvarspolitikken bør også understøtte disse bestræbelser.

Prioriteter

Der er fastlagt seks prioriterede områder i den ajourførte ramme for EU's cyberforsvarspolitik. Hovedfokus for denne politikramme er udvikling af cyberforsvarskapaciteter og beskyttelse af EU's FSFP-kommunikationsnet og -informationsnet. Andre prioriterede områder er: uddannelse og øvelser, forskning og teknologi, civil-militært samarbejde og internationalt samarbejde. På uddannelsesområdet lægges der vægt på styrkelse af medlemsstaternes cyberforsvarsuddannelse og af cyberbevidsthedsuddannelsen for FSFP-kommandovejen. Det er også vigtigt, at cyberdimensionen indgår i tilstrækkeligt omfang i øvelser for at forbedre EU's evne til at reagere på cyberkriser og hybride kriser ved at forbedre beslutningsprocedurerne og tilgængeligheden af information. Cyberspace er et område i hastig udvikling, og ny teknologisk udvikling skal støttes på både det civile og det militære område. Civil-militært samarbejde på cyberområdet er afgørende for at sikre en sammenhængende reaktion på cybertrusler. Sidst, men ikke mindst, kan styrkelse af samarbejdet med internationale partnere bidrage til at øge cybersikkerheden i og uden for EU og til at fremme EU's principper og værdier.

Denne ramme skitserer forslag og muligheder for koordinering mellem relevante EU-institutioner, -organer og -agenturer. Den afspejler også den vigtige rolle, som den private sektor spiller for udvikling af cybersikkerheds- og cyberforsvarsteknologier.

Derudover støtter rammen for EU's cyberforsvarspolitik yderligere cyberforsvarsintegration i Unionens krisestyringsmekanismer, når relevante bestemmelser i EU-traktaten og traktaten om EU's funktionsmåde[9] kan finde anvendelse for at håndtere virkningerne af en cyberkrise.

1. Støtte til udvikling af medlemsstaternes cyberforsvarskapaciteter

Udvikling af cyberforsvarskapaciteter og -teknologier bør tage hensyn til alle aspekter af kapacitetsudvikling, herunder doktrin, ledelse, organisation, personale, uddannelse, industri, teknologi, infrastruktur, logistik og interoperabilitet. Med henblik herpå bør medlemsstaterne intensivere deres indsats for at tilvejebringe effektiv cyberforsvarskapacitet. EU-Udenrigstjenesten, Kommissionen og EDA bør samarbejde og støtte denne indsats.

En løbende vurdering af de svage punkter i de informationsinfrastrukturer, der støtter FSFP-missioner og -operationer, er påkrævet sammen med en næsten tidstro forståelse af beskyttelsens effektivitet. Ud fra en operationel synsvinkel er et af de vigtigste fokusområder for cyberforsvarsaktiviteter at opretholde tilgængeligheden, integriteten og fortroligheden af FSFP-kommunikationsnet og -informationsnet, medmindre andet er specificeret i mandatet for operationerne eller missionerne. Desuden skal EU-Udenrigstjenesten i samarbejde med medlemsstaterne yderligere integrere cyberkapaciteter i FSFP-missioner og -operationer.

Aktører, der står bag ondsindede cyberaktiviteter, skal drages til ansvar for deres handlinger. Det er vigtigt, at EU-medlemsstaterne med støtte fra EU-Udenrigstjenesten fremmer indbyrdes samarbejde om at reagere på ondsindede cyberaktiviteter. Den cyberdiplomatiske værktøjskasse er udviklet til at hjælpe med at opnå en sådan fælles reaktion. EU-Udenrigstjenesten og EDA vil afholde regelmæssige øvelser på grundlag af den cyberdiplomatiske værktøjskasse, hvor EU-medlemsstaterne kan praktisere dette.

[9] Artikel 222 i TEUF og artikel 42, stk. 7, i TEU med behørig hensyntagen til artikel 17 i TEU.

I betragtning af at anvendelsesområdet for cyberforsvar er bredt og forskelligartet, hvis og når det er fastlagt i medlemsstaternes nationale lovgivning og EU-lovgivningen, er der behov for at udvikle en fælles samlet forståelse af anvendelsesområdet for cyberforsvar.

Eftersom militære FSFP-operationer er afhængige af en infrastruktur for kommando, kontrol, kommunikation og computerbehandling (C4), som medlemsstaterne stiller til rådighed, er der behov for en vis grad af strategisk konvergens ved planlægningen af cyberforsvarets behov for informationsinfrastruktur.

På grundlag af arbejdet i EDA's projektgruppe om cyberforsvar med at udvikle cyberforsvarskapaciteter skal EDA og medlemsstaterne:

- anvende CDP og andre instrumenter såsom CARD, der letter og støtter samarbejde mellem medlemsstaterne, med henblik på at forbedre graden af konvergens i planlægningen af cyberforsvarsbehov i medlemsstaterne på det strategiske niveau, navnlig med hensyn til overvågning, situationsbevidsthed, forebyggelse, detektion og beskyttelse, informationsdeling, analysekapacitet inden for kriminalteknik og malware, indhøstede erfaringer, skadesbegrænsning, dynamiske genopretningskapaciteter, decentral datalagring og databackup
- støtte nuværende og fremtidige cyberforsvarsbeslægtede projekter vedrørende sammenlægning og deling af militære operationer (f.eks. inden for kriminalteknik, interoperabilitetsudvikling og fastsættelse af standarder)
- udvikle et sæt standardmålsætninger og -krav, der definerer det mindsteniveau af cybersikkerhed og tillid, som medlemsstaterne skal nå, idet der trækkes på eksisterende ekspertise fra hele EU.

EU-Udenrigstjenesten og EDA skal:

- fremme udvekslinger mellem medlemsstaterne vedrørende de nationale cyberforsvarsdoktriner samt vedrørende cyberforsvarsorienterede rekrutterings-, fastholdelses- og reservistprogrammer.

EDA skal:

- undersøge de forskellige omfang af militære cyberforsvarsbehov i medlemsstaternes nationale lovgivning og bedste praksis. Undersøgelsens hovedformål skal være at udvikle en virksomhedsstruktur for cyberforsvar, der omfatter anvendelsesområde, funktionaliteter og behov, som medlemsstaterne anvender på området i henhold til national lovgivning og EU-lovgivningen.

Medlemsstaterne skal på frivillig basis:

- forbedre samarbejdet mellem deres militære CERT'er for at forbedre forebyggelsen og håndteringen af hændelser
- udnytte PESCO til yderligere at øge samarbejdet om cyberforsvar, herunder nye projekter
- udnytte Den Europæiske Forsvarsfond til i fællesskab at udvikle cyberforsvarskapaciteter
- udvikle en fælles forståelse af anvendelse af bestemmelsen om gensidig bistand på cyberområdet, samtidig med at dens fleksibilitet bevares
- fastlægge grundlæggende cyberforsvarsbehov for informationsinfrastruktur
- udnytte ekspertisen hos ENISA, medlemsstaternes myndigheder samlet i NIS-samarbejdsgruppen og eventuelle andre enheder på EU-plan med ekspertise inden for civil cybersikkerhed, for så vidt forbedring af cyberforsvarskapaciteterne afhænger af civil net- og informationssikkerhedsekspertise.

Medlemsstaterne, EU-Udenrigstjenesten/EU's Militærstab, ESDC og EDA skal:

- overveje at udvikle uddannelse inden for cyberforsvar med henblik på certificering af EU-kampgrupper.

Kommissionen skal i samarbejde med medlemsstaterne:

- overveje cyberforsvar i arbejdsprogrammerne for programmet for udvikling af den europæiske forsvarsindustri og Den Europæiske Forsvarsfond.

2. Styrke beskyttelsen af FSFP-kommunikations- og -informationssystemer, som EU-enheder anvender

Med forbehold af den rolle, som IT-Beredskabsenheden for EU's Institutioner, Organer og Agenturer (CERT-EU) spiller som den centrale EU-struktur for beredskabskoordinering i forbindelse med cyberhændelser for alle Unionens institutioner, organer og agenturer, og inden for rammerne af de relevante regler vedrørende Unionens budget skal EU-Udenrigstjenesten udvikle en passende og selvstændig forståelse af sikkerheds- og netforsvarsanliggender og udvikle sin egen IT-sikkerhedskapacitet. Den skal sigte mod at forbedre modstandsdygtigheden i EU-Udenrigstjenestens FSFP-net med fokus på forebyggelse, detektion, håndtering af hændelser, situationsbevidsthed, informationsudveksling og mekanismer til tidlig varsling.

Beskyttelse af EU-Udenrigstjenestens kommunikations- og informationssystemer og udvikling af sikkerhedskapaciteter inden for informationsteknologi (IT) ledes af EU-Udenrigstjenestens Generaldirektorat for Budget og Administration (BA). Yderligere målrettede ressourcer og støtte skal også ydes af Den Europæiske Unions Militærstab (EUMS), Direktoratet for Krisestyring og Planlægning (CMPD) og Den Civile Planlægnings- og Gennemførelseskapacitet (CPCC). Denne IT-sikkerhedskapacitet skal omfatte både klassificerede og uklassificerede systemer og bliver en integreret del af de eksisterende operationelle enheder.

Der er også behov for at strømline sikkerhedsreglerne for de informationssystemer, som EU's forskellige institutionelle aktører stiller til rådighed under gennemførelsen af FSFP-missioner og -operationer. I den forbindelse kunne en fælles kommandovej overvejes med henblik på at øge modstandsdygtigheden af de net, der bruges til FSFP.

Med henblik på bedre koordinering og for at styrke beskyttelsen og modstandsdygtigheden af kommunikations- og informationssystemer og -net inden for FSFP blev der i 2017 oprettet et internt cyberstyringsråd i EU-Udenrigstjenesten under generalsekretæren.

EU-Udenrigstjenesten/BA skal:

- styrke den IT-sikkerhedsmæssige kapacitet inden for EU-Udenrigstjenesten på grundlag af eksisterende tekniske kapaciteter og procedurer med fokus på forebyggelse, detektion, håndtering af hændelser, situationsbevidsthed, informationsudveksling og mekanismer til tidlig varsling. Strategien for samarbejde med CERT-EU og eksisterende EU-cybersikkerhedskapaciteter skal udbygges yderligere.

EU-Udenrigstjenesten/BA skal sammen med EUMS, MPCC, CMPD og CPCC:

- udvikle sammenhængende IT-sikkerhedspolitik og IT-retningslinjer, idet der også tages hensyn til de tekniske krav til cyberforsvar i en FSFP-sammenhæng i forbindelse med strukturer, missioner og operationer under hensyntagen til de eksisterende samarbejdsrammer og -politikker i EU for at opnå konvergens mellem regler, politikker og organisation.

EU-Udenrigstjenesten/den fælles efterretningsanalysekapacitet (SIAC) skal:

- styrke sin cybertrusselsvurdering og efterretningskapacitet til at identificere nye cyberrisici på grundlag af eksisterende strukturer og foretage regelmæssige risikovurderinger baseret på den strategiske trusselsvurdering og næsten tidstro hændelsesinformation, der koordineres mellem relevante EU-strukturer og gøres tilgængelig på forskellige klassifikationsniveauer.

EU-Udenrigstjenesten/SIAC og CERT-EU skal:

- fremme informationsdeling om cybertrusler i realtid mellem medlemsstater og relevante EU-enheder. Med henblik herpå skal informationsdelingsmekanismer og tillidsskabende foranstaltninger udvikles af relevante nationale og europæiske myndigheder gennem en frivillig tilgang, der bygger på eksisterende samarbejde.

EU-Udenrigstjenesten/EUMS og MPCC skal:

- videreudvikle cyberforsvarskonceptet for militære FSFP-missioner og -operationer og integrere det i planlægningen på strategisk niveau
- i samarbejde med det operative hovedkvarter udarbejde en generel operativ standardcyberprocedure på operationelt niveau.

EU-Udenrigstjenesten/CPCC og CMPD skal:

- videreudvikle og integrere et cyberforsvarskoncept for civile FSFP-missioner i den strategiske planlægning
- styrke civile FSFP-missioners cyberforsvarskapaciteter på grundlag af eksisterende infrastruktur og ved at fremme standardisering og harmonisering af de teknologier, der anvendes inden for FSFP-missioner og -operationer, idet der i relevant omfang drages nytte af CERT-EU's, ENISA's og EDA's ekspertise
- i forbindelse med styrkelsen af den civile FSFP yderligere undersøge muligheden for, at civile FSFP-missioner kan støtte værtsnationer i forbindelse med cybersikkerhed.

EU-Udenrigstjenesten skal:

- videreudvikle fælles krav til militære og civile FSFP-missioner og -operationer
- fremme koordinering af cyberforsvar for at gennemføre mål vedrørende beskyttelse af net, der anvendes af institutionelle aktører i EU, som støtter FSFP, idet der bygges på eksisterende EU-dækkende erfaringer
- regelmæssigt tage ressourcebehov og andre relevante politiske beslutninger op til revision på grundlag af det ændrede trusselsmiljø i samråd med medlemsstaterne og andre EU-institutioner.

3. Fremme af civil-militært samarbejde

Cyberspace er et område i hurtig udvikling: Den teknologiske udvikling skal styrkes ved hjælp af sikkerhedssystemer, både på det civile og det militære område. I det omfang det er muligt, bør der sikres koordinering mellem det civile og det militære område, hvis ensartede teknologiske fremskridt skaber løsninger til både civil og militær brug. I andre tilfælde er de militære kapaciteter og våbensystemer så specifikke, at de ikke kan overføres på civile teknologier. Uden at det berører medlemsstaternes interne organisation og lovgivning kan civil-militært samarbejde på cyberområdet overvejes med henblik på bl.a. udveksling af bedste praksis, informationsudveksling og mekanismer til hurtig varsling, risikovurderinger for håndtering af hændelser og bevidstgørelse samt uddannelse og øvelser.

Forbedring af den civile cybersikkerhed er en vigtig faktor, der bidrager til den overordnede robusthed i net- og informationssikkerheden. NIS-direktivet øger beredskabet på nationalt niveau og styrker samarbejdet på EU-plan mellem medlemsstaterne, både på strategisk og operationelt plan. Dette samarbejde omfatter såvel nationale myndigheder, som fører tilsyn med cybersikkerhedspolitikker, som nationale CERT'er og CERT-EU. Samarbejdet mellem civile og militære CERT'er bør styrkes under behørig hensyntagen til denne udvikling. Formålet med den nye europæiske forordning om cybersikkerhed er at forbedre den europæiske modstandsdygtighed over for cyberangreb og skabe en cybersikkerhedscertificeringsramme for produkter og tjenester og dermed styrke tilliden i den civile digitale sfære.

EDA, Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA), Det Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3) og CERT-EU samt andre relevante EU-organer og -agenturer (inden for deres respektive mandater og uden at overlappe med medlemsstaternes kompetencer) samt medlemsstaterne tilskyndes til yderligere at styrke deres samarbejde på følgende områder:

- udarbejde fælles sikkerheds- og forsvarskompetenceprofiler på cyberområdet baseret på international bedste praksis og certificering anvendt af EU's institutioner, organer og agenturer idet der også tages hensyn til den private sektors certificeringsstandarder
- bidrage til videreudvikling og tilpasning af organisatoriske og tekniske standarder for den offentlige sektors cybersikkerhed og cyberforsvar til brug i forsvars- og sikkerhedssektoren. Om nødvendigt bygge videre på det igangværende arbejde i ENISA og EDA
- udarbejde eller videreudvikle mekanismer og ordninger til udveksling af bedste praksis, navnlig om uddannelse og øvelser samt om forskning og teknologi og andre områder, hvor der er mulighed for civil-militære synergier
- trække på EU's eksisterende erfaringer inden for forebyggelse af cyberkriminalitet, efterforskning og kriminalteknik og øge anvendelsen af disse til at udvikle cyberforsvarskapaciteter.

Medlemsstaterne skal på frivillig basis:

- styrke samarbejdet mellem deres civile og militære CERT'er.

EU-Udenrigstjenesten, Kommissionen og medlemsstaterne skal:

- lade cyberforsvar indgå i EU's krisestyrings- og katastrofehåndteringsprocedurer (via planprocessen).

4. Forskning og teknologi

Operatører af tjenester inden for infrastruktur og informations- og kommunikationsteknologi (IKT) til civile formål og forsvarsformål står over for nogle af de samme udfordringer med hensyn til cybersikkerhed som et resultat af fælles teknologiske og driftsmæssige kapacitetsbehov. Fælles F&T-behov og fælles krav til systemerne forventes at forbedre systemernes interoperabilitet på lang sigt og at reducere udgifterne til udvikling af løsninger. Det er nødvendigt at opnå stordriftsbesparelser for at tackle det stadigt stigende antal trusler og sårbarheder. Dette burde så igen fremme bevarelsen af og væksten inden for en konkurrencedygtig cyberforsvarsindustri i Europa.

Udviklingen af cyberforsvarskapacitet har en vigtig F&T-dimension. Inden for rammerne af forskningsdagsordenen for cyberforsvar har EDA givet et solidt grundlag for prioriteringen af den fremtidige finansiering af F&T inden for den mellemstatslige ramme. Den efterfølgende strategiske forskningsdagsorden udviklet i den relevante ad hoc-arbejdsgruppe under EDA indeholder en kvalificeret prioritering af de cyberrelaterede teknologier, som militæret har behov for, og kortlægger samtidig muligheder for at udvikle og investere i dobbelt anvendelse, både i national, multinational og EU-finansieret sammenhæng.

Udviklingen af teknologiske kapaciteter i Europa til at imødegå trusler og sårbarheder er afgørende. Industrien skal fortsat være den primære drivkraft for cyberforsvarsrelateret teknologi og innovation. Kryptografi, indlejrede systemer, detektion af malware, simulerings- og visualiseringsteknikker, beskyttelse af net- og kommunikationssystemer, identifikations- og autentifikationsteknologi er nogle af de områder, der skal tages fat på. Det er også vigtigt at fremme en konkurrencedygtig europæisk industriforsyningskæde inden for cybersikkerhed ved at støtte inddragelsen af små og mellemstore virksomheder (SMV'er).

Sikringen af Europas evne til at holde trit med internationale konkurrenter inden for teknologiske kapaciteter på cyberområdet afhænger også af vores evne til at fremme banebrydende innovation gennem nationale instrumenter og EU-instrumenter, f.eks. Det Europæiske Innovationsråd.

Med henblik på at lette det civil-militære samarbejde om udvikling af cyberforsvarskapacitet, styrke det europæiske forsvars teknologiske og industrielle basis[10] og bidrage til EU's strategiske autonomi ligeledes på området cyberspace, når og hvis det er nødvendigt, og med partnere overalt, hvor det er muligt**:**

EDA, Kommissionen og medlemsstaterne skal:

- søge at opnå synergieffekter af F&T-bestræbelser i den militære sektor med civile forsknings- og udviklingsprogrammer, navnlig programmer, der vedrører banebrydende innovation, og overveje dimensionen cybersikkerhed og cyberforsvar i forbindelse med gennemførelsen af den forberedende foranstaltning vedrørende forsvarsforskning
- dele forskningsdagsordener for cybersikkerhed (f.eks. Det Europæiske Forsvarsagenturs strategiske forskningsdagsorden for cybersikkerhed) samt køreplaner og tiltag, der udspringer deraf. Med henblik herpå skal der i tæt samarbejde med Kommissionen og medlemsstaterne udvikles en tværsektoriel forskningsdagsorden for cyberforsvar
- bidrage til forbedring af integrationen af cybersikkerheds- og cyberforsvarsdimensioner i programmer, der både har en sikkerheds- og en forsvarsdimension, f.eks. programmet vedrørende forskning i lufttrafikstyring i det fælles europæiske luftrum (SESAR).

[10] Meddelelse "Hen imod en mere konkurrencedygtig og effektiv forsvars- og sikkerhedssektor", COM(2013) 542.

Kommissionen skal:

- overveje at oprette et europæisk kompetencecenter for cybersikkerhed inden for industri, teknologi og forskning med et netværk af nationale koordinationscentre for at støtte teknologiske og industrielle kapaciteter på cybersikkerhedsområdet og øge konkurrenceevnen i Unionens cybersikkerhedsindustri, idet der sikres komplementaritet og undgås overlapninger inden for netværket af kompetencecentre for cybersikkerhed og med andre EU-agenturer. Centret bør i tæt samarbejde og i fuld komplementaritet med Det Europæiske Forsvarsagentur på cyberforsvarsområdet bl.a. få civile og forsvarsrelaterede teknologier og applikationer til at arbejde bedre sammen
- støtte udviklingen af industrielle økosystemer og innovationsklynger, der dækker hele sikkerhedsværdikæden, ved at trække på akademisk viden, SMV'ers innovation og industriproduktion.

Kommissionen skal i samarbejde med medlemsstaterne:

- overveje cyberforsvarsspørgsmål i indkaldelserne fra den forberedende foranstaltning vedrørende forsvarsforskning
- overveje cyberforsvar blandt emnerne i indkalderne fra Den Europæiske Forsvarsfond
- støtte den politiske sammenhæng i EU for at sikre, at de politiske og tekniske aspekter af EU's cyberbeskyttelse forbliver på forkant med den teknologiske innovation og harmoniseres i hele EU (kapacitet til analyse og vurdering af cybertrusler, initiativer til indbygget sikkerhed (security by design), forvaltning af afhængighed af adgang til teknologi osv.).

5. Forbedring af mulighederne for uddannelse og øvelser

Med henblik på at øge beredskabet til at imødegå cybertrusler og udvikle en fælles cyberforsvarskultur i hele EU, der også er til gavn for EU-missioner og -operationer, er der behov for at forbedre og styrke uddannelsesmulighederne inden for cyberforsvar. Det er afgørende, at uddannelsesbudgetterne anvendes effektivt, samtidig med at der skal leveres den bedst mulige kvalitet. Det vil være af afgørende betydning at sammenlægge og dele uddannelse inden for cyberforsvar på europæisk plan.

Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC), EU-Udenrigstjenesten, EDA, Kommissionen og medlemsstaterne skal:

- på grundlag af EDA's analyse af uddannelsesbehovet inden for cyberforsvar og ESDC's erfaringer med uddannelse i cybersikkerhed tilrettelægge FSFP-uddannelse for forskellige målgrupper, herunder EU-Udenrigstjenesten, personale fra FSFP-missioner og -operationer og tjenestemænd fra medlemsstaterne, med henblik på også at imødegå problemer med at fastholde fagkyndigt personale på kort, mellemlang og lang sigt
- foreslå etablering af en cyberforsvarsdialog med medlemsstater, EU-institutioner, tredjelande og andre internationale organisationer samt den private sektor om standarder for uddannelse og certificering
- samarbejde med europæiske uddannelsesudbydere fra den private sektor samt højere læreanstalter for at forbedre kompetencer og kvalifikationer hos personale, der er involveret i FSFP-missioner og -operationer.

ESDC skal:

- videreudvikle platformen for uddannelse, træning, evaluering og øvelse (ETEE) oprettet inden for rammerne af ESDC (ETEE-platformen inden for cybersikkerhed)
- skabe synergier med andre interessenters uddannelsesprogrammer såsom ENISA, Europol, Det Europæiske Politiakademi (Cepol) og NATO's cyberforsvarscenter
- undersøge muligheden for fælles uddannelsesprogrammer i cyberforsvar inden for rammerne af ESDC og NATO, som er åbne for alle EU's medlemsstater, med henblik på at fremme en fælles cyberforsvarskultur.

Kommissionen skal:

- vurdere de muligheder for at styrke uddannelsesmulighederne i medlemsstaterne, som ETEE-platformen inden for cybersikkerhed udpeger.

EDA skal:

- videreudvikle EDA-kurser i samarbejde med ESDC for at opfylde medlemsstaternes behov for uddannelse og øvelser inden for cyberforsvar
- støtte ETEE-platformen inden for cybersikkerhed, bl.a. ved gradvist at integrere de uddannelses-, trænings-, evaluerings- og øvelsesmoduler, der er udviklet inden for rammerne af EDA.

EU-Udenrigstjenesten og medlemsstaterne skal:

- på grundlag af eksisterende standarder og viden følge ESDC's fastlagte certificeringsmekanismer for uddannelsesprogrammerne i tæt samarbejde med de relevante tjenestegrene i EU's institutioner, organer og agenturer og overveje muligheden for at oprette cyberspecifikke moduler inden for rammerne af det militære Erasmusinitiativ.

Der er behov for at forbedre muligheden for cyberforsvarsøvelser for militære og civile FSFP-aktører. Fælles øvelser tjener som middel til at udvikle fælles viden og forståelse for cyberforsvar. Dette vil gøre det muligt for nationale styrker at øge deres beredskab til at arbejde i et multinationalt miljø. Gennemførelsen af fælles cyberforsvarsøvelser vil også skabe interoperabilitet og tillid.

EU-Udenrigstjenesten, EDA, CERT-EU og medlemsstaterne skal fokusere på at fremme cyberforsvarselementer i FSFP og andre øvelser og:

- integrere en cyberforsvarsdimension i de eksisterende øvelsesscenarier for *MILEX* og *Multilayer*
- regelmæssigt afholde strategiske/politiske øvelser såsom *CYBRID 2017* i samarbejde med den EU-ledede parallelle og koordinerede øvelse (PACE) og teknisk-operationelle øvelser såsom *DEFNET*
- om nødvendigt udvikle en særlig FSFP-cyberforsvarsøvelse for EU og undersøge muligheder for koordinering med fælleseuropæiske cyberøvelser såsom *CyberEurope*, der er organiseret af ENISA
- fortsat deltage i andre multinationale cyberforsvarsøvelser såsom *Locked Shields*
- invitere relevante internationale partnere til øvelserne, f.eks. NATO, i overensstemmelse med EU's ramme for øvelsespolitik
- afholde regelmæssige øvelser på grundlag af den cyberdiplomatiske værktøjskasse, som EU-medlemsstaterne kan bruge til at øve sig i at reagere på ondsindede cyberaktiviteter.

6. Styrkelse af samarbejdet med relevante internationale partnere

Inden for rammerne af det internationale samarbejde er der behov for at sikre en dialog med internationale partnere, især NATO og andre internationale organisationer, med henblik på at bidrage til udviklingen af effektive cyberforsvarskapaciteter. Det bør tilstræbes at opnå en øget deltagelse i det arbejde, der udføres inden for rammerne af Organisationen for Sikkerhed og Samarbejde i Europa (OSCE) og De Forenede Nationer (FN), med henblik på at fremme en strategisk ramme for konfliktforebyggelse, samarbejde og stabilitet i cyberspace.

Der er politisk vilje i EU til at udbygge samarbejdet med NATO om cyberforsvar med henblik på udvikling af solide og robuste cyberforsvarskapaciteter som krævet i den fælles erklæring, som formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for Den Nordatlantiske Traktats Organisation undertegnede den 8. juli 2016 i Warszawa. Regelmæssige konsultationer på medarbejderniveau, gensidige briefinger samt eventuelle møder mellem Den Politisk-Militære Gruppe og relevante NATO-komitéer skal bidrage til at undgå unødig overlapning og sikre sammenhæng og komplementaritet mellem bestræbelserne på linje med førnævnte ramme.

EU-Udenrigstjenesten og EDA skal sammen med medlemsstaterne videreudvikle cyberforsvarssamarbejdet mellem EU og NATO, under behørig hensyntagen til den institutionelle ramme og de respektive institutioners selvstændige beslutningstagning, og:

- intensivere de igangværende aktiviteter i forbindelse med gennemførelsen af den fælles erklæring fra formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for Den Nordatlantiske Traktats Organisation
- udveksle bedste praksis for krisestyring og for cyberforsvar i forbindelse med militære og civile missioner og operationer
- arbejde på at skabe sammenhæng i resultaterne i forbindelse med udvikling af behov for cyberforsvarskapacitet, hvor disse overlapper hinanden, navnlig i forbindelse med udvikling af langsigtet cyberforsvarskapacitet
- anvende EDA-samarbejdsrammen med NATO's cyberforsvarscenter yderligere som en indledende platform for styrket samarbejde i multinationale cyberforsvarsprojekter på grundlag af passende vurderinger.

ESDC, EU-Udenrigstjenesten og EDA skal:

- styrke samarbejdet om koncepter for cyberforsvarsuddannelser såvel som øvelser
- sikre gensidig medarbejderdeltagelse i øvelser i overensstemmelse med den aftalte ramme.

CERT-EU skal:

- yderligere udnytte den tekniske aftale mellem CERT-EU og NCIRC (NATO Computer Incident Response Capability) med henblik på at forbedre situationsbevidsthed, informationsudveksling og mekanismer til tidlig varsling og forudse trusler, der kan påvirke begge organisationer.

Med hensyn til andre internationale organisationer og EU's relevante internationale partnere skal EU-Udenrigstjenesten og medlemsstaterne, hvis det er relevant:

- følge den strategiske udvikling og afholde konsultationer om cyberforsvarsemner med internationale partnere (internationale organisationer og tredjelande)
- undersøge mulighederne for samarbejde om cyberforsvarsspørgsmål, herunder med tredjelande, der deltager i FSFP-missioner og -operationer
- i relevante internationale organisationer, navnlig FN, OSCE og ASEAN Regional Forum, fremme anvendelsen af gældende international ret, navnlig FN-pagten i sin helhed, i cyberspace, udviklingen og gennemførelsen af universelle ikkebindende normer for ansvarlig statslig adfærd samt regionale tillidsskabende foranstaltninger mellem stater for at øge gennemsigtigheden og mindske risikoen for fejlfortolkninger af statslig adfærd.

Kommissionen og EU-Udenrigstjenesten skal:

- hvis det er relevant, støtte opbygningen af cyberkapaciteter for EU's partnere gennem det ændrede instrument, der bidrager til stabilitet og fred.

Opfølgning

Efter EU-Udenrigstjenestens samordning af gennemførelsen af rammen for EU's cyberforsvarspolitik bør EU-Udenrigstjenesten/EDA/Kommissionen forelægge en årlig situationsrapport, som omfatter de seks områder, der er beskrevet ovenfor, for Den Politisk-Militære Gruppe med deltagelse af medlemmerne af Den Horisontale Gruppe vedrørende Cyberspørgsmål og for Den Udenrigs- og Sikkerhedspolitiske Komité for at vurdere gennemførelsen af rammen for EU's cyberforsvarspolitik. Hvert halve år gives der desuden en mundtlig redegørelse.

Det er vigtigt, efterhånden som cybertruslen udvikler sig, at nye cyberforsvarsbehov identificeres og efterfølgende medtages i rammen for cyberforsvarspolitikken. Den næste revision af rammen for EU's cyberforsvarspolitik bør forelægges senest medio 2022 i tæt samråd med medlemsstaterne.