EUROPA-
KOMMISSIONEN

UNIONENS HØJTSTÅENDE
REPRÆSENTANT FOR
UDENRIGSANLIGGENDER
OG SIKKERHEDSPOLITIK

Bruxelles, den 13.6.2018
JOIN(2018) 16 final

FÆLLES MEDDELELSE TIL EUROPA-PARLAMENTET, DET EUROPÆISKE RÅD OG RÅDET

Øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler

1. INDLEDNING

Hybride aktiviteter fra statslige og ikkestatslige aktører udgør fortsat en alvorlig og akut trussel mod EU og dens medlemsstater. Bestræbelser på at destabilisere lande ved at undergrave offentlighedens tillid til de offentlige institutioner og ved at anfægte de grundlæggende værdier i samfundene er blevet mere udbredt. Vores samfund står over for en stor udfordring fra dem, der forsøger at skade EU og medlemsstaterne gennem alt fra cyberangreb, der påvirker økonomien og de offentlige tjenester, over målrettede desinformationskampagner og til fjendtlige militære aktioner.

Hybride kampagner er flerdimensionelle og kombinerer tvangsforanstaltninger og undergravende foranstaltninger ved hjælp af både konventionelle og ukonventionelle værktøjer og taktikker (diplomatiske, militære, økonomiske og teknologiske) til at destabilisere modparten. De er udformet, så de er vanskelige at opdage eller placere ansvaret for, og kan anvendes af både statslige og ikkestatslige aktører. Angrebet med nervegift i Salisbury i marts[1] understregede desuden mangfoldigheden af de hybride trusler og de mange taktikker, der nu findes. Som svar fremhævede Det Europæiske Råd[2], at det var nødvendigt at øge kapaciteten i EU og medlemsstaterne til at afsløre, forhindre og reagere på hybride trusler på områder som cybersikkerhed, strategisk kommunikation og efterretningstjenester. Det henledte også særligt opmærksomheden på behovet for modstandsdygtighed over for kemiske, biologiske, radiologiske og nukleare trusler.

Truslerne fra ukonventionelle våben hører til i en kategori for sig på grund af det potentielle omfang af de skader, de kan forårsage. Ud over at være vanskelige at opdage og placere ansvaret for er de komplekse at afhjælpe. Kemiske, biologiske, radiologiske og nukleare trusler, som rækker ud over hybride trusler og også dækker terrortrusler, er også en generel bekymring for det internationale samfund[3], især den voksende risiko for spredning, både geografisk og til ikkestatslige aktører.

Det er overvejende medlemsstaternes ansvar at styrke modstandsdygtigheden over for disse trusler og øge kapaciteten. Men EU's institutioner har allerede truffet en række tiltag for at hjælpe med at styrke den nationale indsats. Dette har omfattet et tæt samarbejde med andre internationale aktører, herunder navnlig Den Nordatlantiske Traktats Organisation (NATO)[4], og dette arbejde kunne uddybe støtten til medlemsstaterne på områder som hurtig reaktion[5].

Denne fælles meddelelse er et svar på Det Europæiske Råds opfordring til at videreføre dette arbejde. Det er en del af en større pakke, der også omfatter den seneste statusrapport om sikkerhedsunionen[6], der gør status over og præsenterer næste skridt i gennemførelsen af handlingsplanen for kemiske, biologiske, radiologiske og nukleare sikkerhedsrisici fra

---

1 For så vidt angår angrebet i Salisbury, konkluderede Det Europæiske Råd den 22. marts 2018, at det "er enigt i vurderingen fra Det Forenede Kongeriges regering, hvorefter det med stor sandsynlighed er Den Russiske Føderation, som er ansvarlig, og at der ikke er nogen plausibel alternativ forklaring."

2 Konklusionerne fra Det Europæiske Råds møde i marts 2018.

3 Herunder De Forenede Nationers Sikkerhedsråd, resolution S/RES/2325 (2016) af 14. december 2016.

4 Imødegåelse af hybride trusler er et af de syv områder for samarbejdet med Den Nordatlantiske Traktats Organisation (NATO), der er nævnt i den fælles erklæring, som blev undertegnet i Warszawa i juli 2016 af formanden for Det Europæiske Råd, formanden for Europa-Kommissionen og generalsekretæren for NATO.

5 G7, der mødtes på et topmøde i Charlevoix i juni 2018, nåede også til enighed om at udvikle en hurtig reaktionsmekanisme for G7 til imødegåelse af trusler mod demokratier: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/.

6 Femtende situationsrapport om indførelsen af en effektiv og ægte sikkerhedsunion, COM(2018) 470.

oktober 2017[7], såvel som den anden statusrapport[8] om gennemførelsen af de 22 tiltag i den fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats[9].

2. EU'S INDSATS

Kommissionen og den højtstående repræsentant har gjort sig vedvarende bestræbelser på at opbygge EU's kapacitet og effektivt støtte medlemsstaterne i at imødegå hybride og kemiske, biologiske, radiologiske og nukleare trusler. Der er allerede opnået konkrete resultater på områder som strategisk kommunikation, situationsbevidsthed, styrket beredskab og modstandsdygtighed og styrket kriseresponskapacitet.

East Stratcom-taskforcen, der blev oprettet efter Det Europæiske Råds møde i marts 2015, er gået forrest med arbejdet med at forudsige, spore og imødegå desinformation fra udenlandske kilder. Dens ekspertanalyser og offentlige produkter[10] har i høj grad øget kendskabet til konsekvenserne af russisk desinformation. I løbet af de seneste to år har den afsløret over 4 000 individuelle sager om desinformation, hvoraf mange er direkte rettet mod Europa. I sit arbejde har East Stratcom-taskforcen ligeledes fokuseret på at forbedre formidlingen af positiv kommunikation med øget udbredelse i de østlige nabolande. Efter denne succes er der blevet oprettet to andre taskforcer med forskelligt geografisk fokus – en taskforce for det vestlige Balkan og en dedikeret sydlig taskforce for den arabisktalende verden.

Der er taget vigtige skridt til at opbygge de strukturer, der er nødvendige for at forbedre situationskendskabet og understøtte beslutningstagningen. Den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler blev oprettet inden for EU-Udenrigstjenestens Efterretningsanalysecenter i 2016. Den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler modtager og analyserer klassificerede og offentlige oplysninger fra forskellige interessenter vedrørende hybride trusler. Til dato er der udarbejdet over 100 vurderinger og briefinger, som er delt inden for EU og blandt medlemsstaterne til brug for EU's beslutningsproces. Den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler arbejder tæt sammen med Det Europæiske Center for Imødegåelse af Hybride Trusler i Helsinki. Centret blev oprettet i april 2017 for at fremme en strategisk dialog og udføre forskning og analyser vedrørende hybride trusler og har nu udvidet sin medlemskreds til 16 lande[11] og får fuld støtte fra EU.

Der er ligeledes taget vigtige skridt til at styrke beredskabet og modstandsdygtigheden, navnlig mod kemiske, biologiske, radiologiske og nukleare trusler. I de seneste seks måneder er der gjort en stor indsats for at identificere mangler i beredskabet for kemiske, biologiske, radiologiske og nukleare sikkerhedshændelser, navnlig hvad angår påvisning af kapacitet til at hjælpe med at forebygge kemiske, biologiske, radiologiske og nukleare angreb. På Kommissionens initiativ foretog et konsortium af nationale eksperter en analyse af manglerne i udstyret til opdagelse af forskellige typer af kemiske, biologiske, radiologiske og nukleare scenarier. Rapporten om mangelanalysen er blevet delt med medlemsstaterne og giver dem mulighed for at træffe informerede beslutninger om

---

7 COM(2017) 610 final.

8 Fælles rapport fra Kommissionen om gennemførelsen af den fælles ramme for imødegåelse af hybride trusler (juli 2017-juli 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 Se www.euvsdisinfo.eu.

11 Af de nuværende 16 medlemmer er de 14 EU-medlemsstater: Tjekkiet, Danmark, Estland, Finland, Frankrig, Tyskland, Italien, Letland, Litauen, Nederlandene, Polen, Spanien, Sverige og Det Forenede Kongerige. Initiativet til oprettelsen heraf kommer fra den fælles ramme for imødegåelse af hybride trusler. Centret er også blevet aktivt støttet af EU og NATO inden for rammerne af deres samarbejde.

opdagelsesstrategier og træffe konkrete foranstaltninger til afhjælpning af de identificerede mangler.

Dette arbejde er blevet bakket op gennem øvelser, der tester graden af fremskridt. Den parallelle og koordinerede øvelse i 2017 (PACE17) med NATO har gjort det muligt at foretage en detaljeret undersøgelse af EU's indsatskapacitet over for store hybride kriser. Øvelsen er den hidtil mest omfangsrige af sin art og testede ikke blot EU's "hybride spilleregler", de forskellige EU-indsatsordninger og deres evne til at interagere effektivt med hinanden, men også, hvordan EU's reaktion på hybride trusler spillede sammen med NATO's indsats. En 2018-øvelse er ved at blive planlagt med det formål ikke blot at etablere den som en årlig begivenhed, men også for at hjælpe medlemsstaterne med at styrke deres hybride kriseberedskabskapacitet.

Disse konkrete tiltag illustrerer, hvordan de politiske rammer i EU er begyndt at bære frugt: De seneste to år har været skueplads for en række rammer, som skal lede og målrette EU's arbejde.

I den *fælles ramme for imødegåelse af hybride trusler – Den Europæiske Unions indsats* fra april 2016[12] blev der opfordret til en tværministeriel tilgang med 22 indsatsområder, der kan bidrage til at imødegå **hybride trusler** og styrke modstandsdygtigheden hos EU og medlemsstaterne samt hos internationale partnere. De fleste foranstaltninger, der er defineret i den fælles ramme, har fokus på at forbedre situationskendskabet og opbygge modstandsdygtighed med bedre kapacitet til at reagere. De spænder fra at styrke EU's efterretningsanalysekapacitet til at styrke beskyttelsen af kritisk infrastruktur og cybersikkerhed til at bekæmpe radikalisering og voldelig ekstremisme. Cyberrelaterede trusler og cyberangreb er også kernen i den fælles ramme. Den anden statusrapport om gennemførelsen af den fælles ramme, der blev vedtaget sideløbende med denne fælles meddelelse, viser konkrete fremskridt for disse foranstaltninger og bekræfter styrkelsen og udbygningen af EU's bestræbelser på at imødegå hybride trusler[13].

Med hensyn til **cybersikkerhed** var den 9. maj 2018 en vigtig milepæl som frist for alle EU's medlemsstater til at gennemføre det første EU-dækkende og retligt bindende regelsæt om IT-sikkerhed, nemlig direktivet om sikkerhed for net -og informationssystemer. Dette er en vigtig del af den bredere tilgang, der er fastlagt i den *fælles meddelelse om modstandsdygtighed, forsvar og afskrækkelse*: *opbygning af en stærk cybersikkerhed for EU*[14] fra september 2017 med vidtrækkende konkrete foranstaltninger til at give et kraftigt skub til EU's cybersikkerhedsstrukturer og -kapaciteter. Fokus var her på at opbygge EU's modstandsdygtighed over for cyberangreb og styrke EU's kapacitet inden for cybersikkerhed, skabe en effektiv strafferetlig indsats og styrke global stabilitet gennem internationalt samarbejde. Dette var ledsaget af et forslag til en lov om cybersikkerhed for at styrke støtten på EU-plan[15] og er blevet bakket op med en række forslag, der skal videreføres til gennemførelse (se nedenfor).

Desinformation skader vores demokratier ved at hæmme borgernes evne til at træffe informerede beslutninger og deltage i den demokratiske proces. Internettet har drastisk øget mængden og mangfoldigheden af de nyheder, borgerne har adgang til. Men nye teknologier kan anvendes til udbredelse af desinformation i et hidtil uset omfang og med en hidtil uset hastighed og kan målrettet så mistillid og skabe større spændinger i samfundet. Kommissionens *meddelelse om bekæmpelse af desinformation på internettet:*

---

13 For den første gennemførelsesrapport (juli 2017): JOIN(2017) 30 final.
14 JOIN(2017) 450 final.
15 COM(2017) 477, se nedenfor.

en europæisk tilgang[16] indeholdt en europæisk tilgang til at løse problemet med desinformation ved at opfordre forskellige interessenter, navnlig onlineplatforme, men også medieselskaber, til at iværksætte tiltag. Disse tiltag omfatter en bred vifte af områder, herunder øget gennemsigtighed, onlineplatformes troværdighed og ansvarlighed, mere robuste og modstandsdygtige valgprocesser, fremme af uddannelse og mediekendskab, støtte af kvalitetsbetonet journalistik og imødegåelse af desinformation gennem strategisk kommunikation. De første konkrete skridt omfatter en adfærdskodeks om desinformation, som skal udarbejdes af et multiinteressentforum om desinformation og et netværk af faktatjekkere, som skal være på plads senest til sommer. Det første møde i EU's multiinteressentforum om desinformation blev afholdt den 29. maj 2018, hvor der blev aftalt de nødvendige skridt til at vedtage kodeksen i juli 2018. Kommissionen vil inden udgangen af 2018 vurdere de fremskridt, der er gjort med hensyn til at tackle problemet og afgøre, om der er behov for at gøre en yderligere indsats på dette område. De planlagte aktiviteter vil hænge sammen med og supplere aktiviteterne i East Stratcom-taskforcen.

For så vidt angår **kemiske, biologiske, radiologiske og nukleare risici**, foreslog Kommissionen i sin *handlingsplan*[17] fra oktober 2017 23 konkrete tiltag og foranstaltninger, der tager sigte på en bedre beskyttelse af borgere og infrastrukturer mod disse trusler, herunder gennem et tættere samarbejde mellem EU og dens medlemsstater og med NATO. Som led i foranstaltningerne i sikkerhedsunionen for at forbedre beskyttelsen mod og modstandsdygtigheden over for terrorisme fulgte den en forbyggende tilgang baseret på den begrundelse, at kemiske, biologiske, radiologiske og nukleare risici havde en lav sandsynlighed, men en stor og vedvarende effekt i tilfælde af et angreb. I mellemtiden viser angrebet i Salisbury samt stigende bekymring over terrorangreb og muligheden for at anvende kemiske, biologiske, radiologiske og nukleare materialer både i og uden for EU[18], at truslen fra kemiske, biologiske, radiologiske og nukleare stoffer er reel. Dette styrker yderligere det presserende behov for at gennemføre handlingsplanen fuldt ud. Det følger en samlet risikotilgang med fokus på fire mål: at reducere tilgængeligheden af kemiske, biologiske, radiologiske og nukleare materialer, at sikre et mere solidt beredskab og en indsats i forbindelse med kemiske, biologiske, radiologiske og nukleare sikkerhedshændelser, at opbygge stærkere interne og eksterne forbindelser inden for kemisk, biologisk, radiologisk og nuklear sikkerhed med centrale regionale og internationale partnere i EU og at fremme kendskabet til kemiske, biologiske, radiologiske og nukleare risici. Detaljerede oplysninger om konkrete fremskridt i gennemførelsen af handlingsplanen er fremlagt i den seneste statusrapport om sikkerhedsunionen, der blev vedtaget parallelt med denne fælles meddelelse.

For at effektivisere bestræbelserne på at imødegå hybride trusler og styrke budskabet om sammenhold blandt EU's medlemsstater og NATO's allierede er samarbejdet om bekæmpelse af hybride trusler blevet defineret som et centralt område for **samarbejdet mellem EU og NATO** som beskrevet i den *fælles erklæring fra Warszawa*[19] i juli 2016. Næsten en tredjedel af alle de nuværende fælles forslag til samarbejde fokuserer på hybride trusler[20]. Øvelserne og "EU-drejebogen"[21], der er beskrevet ovenfor, udbygges med et uddybet samarbejde i år.

---

16 COM(2018) 236 final.

17 COM(2017) 610 final.

18 Europol, Terrorism Situation and Trend report (TE-SAT) 2017, s. 16, der findes på: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Se også erklæringerne fra generaldirektøren for OPCW: www.globaltimes.cn/content/1044644.shtml.

19 Den erklæring, der blev undertegnet af Kommissionens formand Jean-Claude Juncker, EU-formand Donald Tusk og NATO's generalsekretær Jens Stoltenberg, udgør det nuværende grundlag for samarbejdet mellem EU og NATO.

20 15283/16 og 14802/17.

21 SWD(2016) 227 final.

3. INTENSIVERING AF REAKTIONEN PÅ NYE TRUSLER

3.1. Situationskendskab – bedre kapacitet til at påvise hybride trusler

Bestræbelser på at bekæmpe og reagere på hybride trusler skal underbygges af en kapacitet til at påvise tidlige ondsindede hybride aktiviteter og kilder, såvel interne som eksterne, og forstå de mulige forbindelser mellem ofte tilsyneladende uforbundne begivenheder. Med henblik herpå er det vigtigt at gøre brug af alle tilgængelige oplysninger, herunder oplysninger fra åbne kilder.

Den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler blev oprettet som et vigtigt aktiv i EU-Udenrigstjenesten som et enkelt fokuspunkt for analyser af hybride trusler, men den har brug for den fornødne ekspertise til at håndtere hele spektret af hybride trusler, herunder kemiske, biologiske, radiologiske og nukleare trusler samt efterretningstrusler. En bredere ekspertise vil øge støtten til EU's fremtidige krisesituationer ved at tilbyde mere komplette civile og militære efterretningsprodukter inden for disse områder. Dette kan suppleres af medlemsstaternes indsats for at øge de nationale efterretningstjenesters bidrag til den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler og yderligere forbedre muligheden for, at det etablerede net af nationale kontaktpunkter for den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler kan give og behandle tidskritiske oplysninger. Et andet skridt ville være, at medlemsstaterne overvejer at øge deres nationale efterretningstjenesters bidrag til EU's Efterretningsanalysecenter (INTCEN) for at muliggøre mere dybtgående analyser af potentielle trusler.

Fremtidige skridt

- Den højtstående repræsentant vil udvide den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler med specialiserede kemiske, biologiske, radiologiske og nukleare, efterretningsmæssige samt cyberanalytiske komponenter. Medlemsstaterne opfordres til at øge deres efterretningstjenesters bidrag til den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler for at kunne analysere eksisterende og nye hybride trusler.

- Kommissionen vil i samarbejde med den højtstående repræsentant færdiggøre arbejdet med sårbarhedsindikatorer for at give medlemsstaterne mulighed for bedre at vurdere de potentielle hybride trusler i forskellige sektorer. Dette arbejde vil også støtte EU's analyse af hybride tendenser.

3.2. Styrkede tiltag mod kemiske, biologiske, radiologiske og nukleare trusler

Handlingsplanen fra oktober 2017 om håndtering af kemiske, biologiske, radiologiske og nukleare sikkerhedsrisici udstikker rammerne for de tiltag, der skal styrke modstandsdygtighed, beredskab og koordinering på EU-plan. Tiltagene i handlingsplanen omfatter en række foranstaltninger, som skal støtte medlemsstaterne ved at samle ekspertise og fælles kapacitetsopbygning, udveksle viden og bedste praksis og intensivere det operationelle samarbejde. Medlemsstaterne og Kommissionen bør arbejde sammen for at gennemføre handlingsplanen fuldt ud som en hastesag. Desuden bør Unionen med udgangspunkt i de fremskridt, der allerede er gjort med hensyn til mangelanalysen af opdagelsesmulighederne og udveksling af bedste praksis i den nyoprettede rådgivende gruppe om kemisk, biologisk, radiologisk og nuklear sikkerhed, tage yderligere skridt til at tackle udvikling og nye trusler. Dette gælder navnlig kemiske trusler. Efter eksemplet med

at arbejde for at begrænse adgang til udgangsstoffer til eksplosivstoffer[22] er EU nødt til hurtigt at træffe operationelle foranstaltninger for bedre at kontrollere adgangen til kemikalier i højrisikogruppen og optimere evnen til at påvise sådanne materialer så tidligt som muligt. Medlemsstaterne bør også overveje at foretage en yderligere mangelanalyse og kortlægning på EU-plan, f.eks. af den kemiske, biologiske, radiologiske og nukleare modstandsdygtighed samt dekontamineringsaktiver og tilgange. Forberedelse og håndtering af konsekvenserne af kemiske, biologiske, radiologiske og nukleare angreb kræver et styrket samarbejde og koordinering mellem medlemsstaterne, herunder civilbeskyttelsesmyndigheder. EU's civilbeskyttelsesordning kan spille en nøglerolle i denne proces med henblik på at styrke EU's kollektive kapacitet til at forberede sig og reagere.

Internationalt samarbejde er ligeledes et vigtigt element i dette arbejde, og EU kan bygge videre på forbindelserne med de regionale kemiske, biologiske, radiologiske og nukleare ekspertisecentre, herunder søge synergier med NATO, og programmerne for forebyggelse, beredskab og reaktion på naturkatastrofer og menneskeskabte katastrofer for syd og øst[23].

Fremtidige skridt

- EU bør undersøge mulige foranstaltninger til at sikre overholdelse af internationale regler og standarder i forhold til brug af kemiske våben, herunder gennem en eventuel specifik EU-sanktionsordning om kemiske våben.

- For at komme videre med den kemiske, biologiske, radiologiske og nukleare handlingsplan vil Kommissionen arbejde sammen med medlemsstaterne om at tage følgende skridt inden udgangen af 2018:
  - udarbejde en liste over kemiske stoffer, som udgør en særlig trussel, som grundlag for den operationelle indsats for at reducere deres tilgængelighed
  - etablere en dialog med private aktører i forsyningskæden om at arbejde sammen om at håndtere nye trusler fra kemikalier, som kan bruges som udgangsstoffer
  - fremskynde en revision af trusselsscenarier og en analyse af eksisterende metoder til at forbedre opdagelse af kemiske trusler, med det formål at udvikle operationelle retningslinjer til medlemsstaterne for at intensivere deres sporingskapacitet.

- Medlemsstaterne bør udarbejde oversigter over lagre af vigtige medicinske modforanstaltninger, laboratorie-, behandlings- og andre kapaciteter. Kommissionen vil i samarbejde med medlemsstaterne regelmæssigt kortlægge tilgængeligheden af disse lagre i hele EU med henblik på at øge deres adgang til og hurtig udbredelse i tilfælde af angreb.

[22] Som en del af arbejdet i sikkerhedsunionen med at lukke det rum, hvor terrorister og kriminelle opererer, har Kommissionen truffet håndfaste tiltag til at mindske adgangen til udgangsstoffer til eksplosivstoffer, der kan misbruges til at fremstille hjemmelavede sprængstoffer. I oktober 2017 fremsatte Kommissionen en henstilling om øjeblikkelige foranstaltninger med henblik på at forebygge misbrug af udgangsstoffer til eksplosivstoffer på grundlag af de gældende regler (henstilling C(2017) 6950 final). Med udgangspunkt deri vedtog Kommissionen i april 2018 et forslag om at revidere og styrke den eksisterende forordning 98/2013 om markedsføring og brug af udgangsstoffer til eksplosivstoffer (COM(2018) 209 final).

[23] I de østlige og sydlige nabolande organiseres der undervisning og øvelser i civilbeskyttelse under regionalprogrammerne for forebyggelse, beredskab og reaktion på naturkatastrofer og menneskeskabte katastrofer.

3.3. **Strategisk kommunikation – sammenhængende formidling af oplysninger**

En vigtig udfordring i forbindelse med hybride trusler er at bevidstgøre og oplyse offentligheden om at skelne oplysninger fra desinformation. På grundlag af erfaringerne med East Stratcom-taskforcen, den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler og Det Europæiske Center for Imødegåelse af Hybride Trusler samt andre bestræbelser fra Kommissionen[24] vil Kommissionen og den højtstående repræsentant videreudvikle og forbedre EU's kapacitet inden for strategisk kommunikation ved at sikre systematisk samarbejde og sammenhæng mellem de eksisterende strukturer. Dette vil blive yderligere udvidet til at omfatte andre EU-institutioner og medlemsstaterne, herunder ved hjælp af den bebudede sikre onlineplatform for desinformation.

Bedre koordinering og samarbejde om strategisk kommunikation på tværs af de forskellige EU-institutioner med medlemsstaterne og med partnere og internationale organisationer vil være af afgørende betydning og kræver forberedelse og erfaring, før der kan reageres på kriser i realtid.

Valgperioder har vist sig at være særligt strategiske og følsomme mål for cyberangreb og onlineomgåelse af traditionelle ("offline") garantier og regler såsom stilleperioder, gennemsigtige finansieringsregler og ligebehandling af ansøgere. Dette har omfattet angreb mod valginfrastrukturer og kampagne-IT-systemer samt politisk motiverede massedesinformationskampagner online og cyberangreb fra tredjelande med det formål at miskreditere og aflegitimere demokratiske valg. Flere arbejdsområder videreføres på EU-plan for at øge bevidstheden i medlemsstaterne i forbindelse med forberedelserne og reaktionerne på disse trusler. I Rådet vil medlemsstaternes cybersikkerhedsmyndigheder[25] udstede frivillige retningslinjer og definere fælles bedste praksis til håndtering af cybersikkerhed inden for valgteknologi i hele valgets livscyklus. Dette omfatter informationssystemer og IKT-løsninger, der anvendes til registrering af vælgere og kandidater og til at indsamle og optælle stemmer og offentliggøre resultater, samt hjælpesystemer, som er knyttet direkte til lovligheden af valgresultatet.

Der er også behov for at sikre hurtige, pålidelige og ensartede oplysninger til offentligheden i tilfælde af hybride angreb. Enhver kemisk, biologisk, radiologisk og nuklear hændelse eller tilsvarende forårsager et offentligt ramaskrig, når borgerne kræver hurtige svar. Strategiske budskaber har en vigtig rolle, også mellem internationale organisationer, som måske udøver deres beredskabsplaner særskilt.

---

[24] Kommissionens repræsentationer er f.eks. også aktive inden for faktatjek og fjernelse af myter. Adskillige har udviklet lokalt tilpassede instrumenter som f.eks. *Les Décodeurs de l'Europe* i Frankrig, UE Vero Falso i Italien, en offentlig europæisk tegnekonkurrence om fjernelse af myter i Østrig, en lignende tegneserie i Rumænien og Det Forenede Kongeriges repræsentationens Euromyths A-Z. Flere sådanne projekter er under udarbejdelse.

[25] Inden for rammerne af den samarbejdsgruppe, der er nedsat i henhold til direktivet om sikkerheden af net- og informationssystemer.

Fremtidige skridt

- EU-Udenrigstjenesten og Kommissionen vil inden for rammerne af deres respektive beføjelser arbejde sammen om at etablere et mere struktureret samarbejde om strategisk kommunikation for at forhindre udbredelse af desinformation både i og uden for EU og for at afskrække produktion af fjendtlig desinformation og hybrid indblanding fra udenlandske regeringer.

- Kommissionen vil i efteråret afholde arrangementer på højt niveau sammen med medlemsstaterne og relevante interessenter, herunder kollokviet om grundlæggende rettigheder, som arbejder for demokrati, for at fremme bedste praksis og retningslinjer for at forhindre, afhjælpe og reagere på cybertrusler og trusler om desinformation i forbindelse med valg.

- Den højtstående repræsentant og Kommissionen vil se på mulighederne for bedre at kunne støtte, i form af værktøjer og ressourcer, det arbejde, som udføres af de tre Stratcom-taskforcer, for at sikre at EU's indsats er tilstrækkelig i forhold til de komplekse desinformationskampagner, der gennemføres af fjendtlige aktører.

3.4. **Opbygning af modstandsdygtighed og afskrækkelse i cybersikkerhedsbranchen**

Cybersikkerhed er afgørende for både vores velstand og sikkerhed. I takt med at vores dagligdag og økonomier bliver mere og mere afhængige af digitale teknologier, bliver vi mere og mere sårbare.

Effektiv cybersikkerhed i EU i dag er hæmmet af utilstrækkelige investeringer og utilstrækkelig koordinering. EU forsøger nu at afhjælpe dette ved at opbygge kapacitet gennem støtteforanstaltninger, bedre koordinering og nye strukturer for at fremme teknologi og udbredelse inden for cybersikkerhed[26]. Med direktivet om sikkerheden af net- og informationssystemer[27] indførtes et minimumsniveau for sikkerheden i net- og informationssystemer i hele EU. Det er vigtigt, at direktivet gennemføres fuldt ud i alle medlemsstater for at øge modstandsdygtigheden over for cyberangreb: Dette er et vigtigt første skridt. Med den generelle forordning om databeskyttelse indføres en forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed. Andre nøgleforanstaltninger omfatter et styrket og moderniseret europæisk Agentur for Cybersikkerhed og en europæisk ramme for certificering af IKT-produkter og -tjenester[28] for at opbygge forbrugernes tillid. Arbejdet med at bistå netværket af medlemsstaternes kompetencecentre med at stimulere udviklingen og anvendelsen af cybersikkerhedsløsninger og supplere bestræbelserne på at opbygge kapacitet på dette område på EU-plan og nationalt plan er også i gang. Dette vil trække på arbejdet i programmet om det digitale Europa, som blev forelagt af Kommissionen den 6. juni[29], og som nyprioriterer EU's investeringer i cybersikkerhed.

---

[26] Som led i styrkelsen af innovation i Europas regioner blev der i december 2017 lanceret et nyt interregionalt pilotprojekt, der samler EU's regioner om at optrappe arbejdet med cybersikkerhed.

[27] 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.

[28] COM(2017) 477 final.

[29] Forslag til forordning om oprettelse af programmet om det digitale Europa i perioden 2021-2027, COM(2018) 434.

Samtidig blev det i en henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser ("planen")[30] beskrevet, hvordan samarbejdet bør fungere mellem medlemsstaterne og de forskellige EU-aktører, som reagerer på et større grænseoverskridende cyberangreb. Det blev understreget, at situationskendskab er afgørende for at sikre en effektiv koordination på teknisk, operationelt og strategisk/politisk niveau. Den samarbejdsgruppe, der er nedsat i henhold til direktivet om sikkerhed for net- og informationssystemer, arbejder også for at fremme udveksling og deling af oplysninger mellem berørte parter og udvikle en fælles klassificering til at beskrive en hændelse. Denne tilgang vil blive testet i kommende øvelser. En strategisk analyse af eksisterende og nye cybertrusler baseret på bidrag fra medlemsstaternes efterretningstjenester leveres af den centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler.

Rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse") var et stort skridt fremad på det operationelle plan og beskriver foranstaltningerne under den fælles udenrigs- og sikkerhedspolitik, herunder restriktive foranstaltninger, der kan anvendes til at styrke EU's reaktion på aktiviteter, der skader de politiske, sikkerhedsmæssige og økonomiske interesser. Jo mere denne anvendes fuldt ud af medlemsstaterne, jo mere vil den fungere som et effektivt afskrækkende middel. I april vedtog Rådet for Udenrigsanliggender konklusioner om ondsindede cyberaktiviteter, som på det kraftigste fordømte ondsindet anvendelse af informations- og kommunikationsteknologier, herunder i WannaCry- og NotPetya-angrebene, der har forårsaget betydelige skader og økonomisk tab i og uden for EU.

EU og medlemsstaterne er nødt til at forbedre deres kapacitet til at placere ansvaret for cyberangreb, ikke mindst gennem øget udveksling af efterretningsoplysninger. Placering af ansvaret ville afskrække potentielle gerningsmænd og øge chancerne for, at de ansvarlige bliver stillet til ansvar. At øge den afskrækkende virkning er et afgørende mål for Kommissionens strategi til forbedring af cybersikkerheden. Kommissionens nylige forslag, der sigter mod at forbedre den grænseoverskridende indsamling af elektronisk bevismateriale i straffesager, vil også i betydelig grad styrke retshåndhævende myndigheders evne til at efterforske og retsforfølge IT-kriminalitet.

Det er nødvendigt med en fælles og omfattende tilgang for at opnå stor cyberrobusthed. Dette kræver mere robuste og effektive strukturer til fremme af cybersikkerhed og til at reagere på cyberangreb i medlemsstaterne, også i EU's egne institutioner, agenturer, delegationer, missioner og operationer: Manglen på et fælles sikret kommunikationsnet på tværs af de europæiske institutioner er en væsentlig svaghed. Bevidstheden om cybersikkerhed i EU's institutioner og hos deres personale bør øges med en forbedret sikkerhedskultur og mere intensiv undervisning.

[30] C(2017) 6100.

Fremtidige skridt

- Europa-Parlamentet og Rådet bør fremskynde arbejdet med at afslutte forhandlinger om forslag til cybersikkerhedsaftaler inden årets udgang og hurtigt blive enige om den foreslåede lovgivning om indsamling af elektronisk bevismateriale.

- Kommissionen og den højtstående repræsentant vil arbejde tæt sammen med medlemsstaterne om at fremme cyberaspekterne af EU's krisestyrings- og indsatsmekanismer. Medlemsstaterne opfordres til at fortsætte deres arbejde med at placere ansvaret for cyberangreb og den praktiske anvendelse af den cyberdiplomatiske værktøjskasse med henblik på at intensivere den politiske reaktion på cyberangreb.

- Som reaktion på behovet for at intensivere vores cyberforsvarskapacitet etableres der en målrettet uddannelsesplatform, som skal hjælpe med at koordinere uddannelsesmulighederne inden for cyberforsvar, som tilbydes af medlemsstaterne. Det tilstræbes at indgå i synergier med lignende bestræbelser i NATO.

3.5. Opbygning af modstandsdygtighed mod fjendtlig efterretningsvirksomhed

At modvirke fjendtlig efterretningsvirksomhed kræver først og fremmest bedre og mere effektiv koordinering mellem medlemsstaterne i overensstemmelse med relevante EU-regler og -ordninger og nationale regler og ordninger. Det er imidlertid også vigtigt at øge EU-institutionernes kapacitet til at imødegå den voksende trussel fra en sådan aktivitet, der er specifikt rettet mod institutionerne, og opbygge en sikkerhedskultur, der understøttes af bedre uddannelse og fysisk sikkerhed. Institutionerne kan også arbejde sammen med medlemsstaterne om at opbygge et mere robust EU-akkrediteringssystem. Et sådant system vil være baseret på proaktiv rapportering og skabe større bevidsthed blandt medlemsstater og EU-institutioner om eventuelle fjendtlige aktører, navnlig dem, der allerede er identificeret af medlemsstaterne.

Koordinering blandt medlemsstaterne og mellem medlemsstaterne og andre relevante internationale organisationer, navnlig NATO, vil bidrage til at udnytte efterretningstjenesterne til at modvirke fjendtlig aktivitet i EU. Et eksempel på et område, der kan drage fordel af øget koordinering mellem medlemsstaterne, er investeringsscreening på grundlag af en forordning[31] foreslået af Kommissionen i september 2017 om screening af udenlandske direkte investeringer i medlemsstaterne af hensyn til den offentlige sikkerhed eller orden. Øget koordinering mellem medlemsstaterne vil være lige så vigtigt for kontrollen med finansielle transaktioner, eftersom fjendtlige efterretningstjenester i stigende grad finansierer deres aktive foranstaltninger over for EU gennem omstændelige finansielle ordninger.

[31] Forslag til Europa-Parlamentets og Rådets forordning om et regelsæt for screening af udenlandske direkte investeringer i Den Europæiske Union, COM(2017) 487.

Fremtidige skridt

- EU-Udenrigstjenesten og Kommissionen vil indføre forbedrede praktiske foranstaltninger til at opretholde og udvikle EU's evne til at interagere med medlemsstaterne med henblik på at modvirke fjendtlig efterretningsvirksomhed, der er specifikt rettet mod institutionerne.

- Den styrkede centrale EU-enhed for analyse og udveksling af oplysninger om hybride trusler vil blive suppleret af efterretningseksperter, som kan levere detaljerede analyser og briefinger om arten af sandsynlig fjendtlig efterretningsvirksomhed mod enkeltpersoner og institutioner.

- Europa-Parlamentet og Rådet bør fremskynde arbejdet med at afslutte forhandlingerne om forslaget om investeringsscreening inden årets udgang.

4. KONKLUSION

EU er meget opmærksom på hybride og kemiske, biologiske, radiologiske og nukleare trusler. Hændelsen i marts i Det Forenede Kongerige understregede det brede spektrum af hybrid krigsførelse og det særlige behov for modstandsdygtighed over for kemiske, biologiske, radiologiske og nukleare trusler.

Kommissionen og den højtstående repræsentant har vedtaget og foreslået en række initiativer til at imødegå de udfordringer, som de hybride trusler udgør. Kommissionen fremskynder desuden gennemførelsen af handlingsplanen fra 2017 for at styrke beredskabet over for kemiske, biologiske, radiologiske og nukleare sikkerhedsrisici.

Denne fælles meddelelse har til formål at orientere Det Europæiske Råd om det arbejde, som allerede pågår, og identificere områder, hvor indsatsen bør intensiveres, for at uddybe og styrke EU's væsentlige bidrag til at imødegå disse trusler. Det er nu op til medlemsstaterne, Kommissionen og den højtstående repræsentant at sikre en hurtig opfølgning.