EUROPEISKA
KOMMISSIONEN

UNIONENS HÖGA
REPRESENTANT FÖR
UTRIKES FRÅGOR OCH
SÄKERHETSPOLITIK

Bryssel den 13.9.2017
JOIN(2017) 450 final

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET

Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU

1. INLEDNING

Cybersäkerhet är av avgörande betydelse både för vårt välstånd och för vår säkerhet. Allteftersom vår vardag och våra ekonomier blir alltmer beroende av digitala tekniker, blir vi också alltmer utsatta. Cybersäkerhetsincidenterna blir mer varierande, i fråga om vilka som är ansvariga och vad de vill åstadkomma. Skadliga cyberaktiviteter hotar inte bara våra ekonomier och den digitala inre marknadens drivkraft, utan även själva grunden för våra demokratier, friheter och värderingar. Vår framtida säkerhet beror på om vi kan omvandla vår förmåga att skydda EU mot cyberhot: både civil infrastruktur och militär kapacitet är beroende av säkra digitala system. Europeiska rådet bekräftade detta vid sitt toppmöte i juni 2017[1], och det bekräftas även i den globala strategin för EU:s utrikes- och säkerhetspolitik[2].

Riskerna ökar exponentiellt. Undersökningar visar att cyberbrottslighetens ekonomiska inverkan har ökat femfaldigt från 2013 till 2017, och att den kan fyrdubblas till 2019[3]. Ransomware[4] har ökat särskilt mycket, och den senaste tidens angrepp[5] visar på en dramatisk ökning av cyberbrottsligheten. Ransomware är dock inte det enda hotet.

Cyberhoten kommer från både icke-statliga och statliga aktörer. De är ofta kriminella, med vinstsyfte, men kan även vara politiska och strategiska. Brottshotet förvärras av den otydliga gränsen mellan cyberbrottslighet och ”traditionell” brottslig verksamhet, eftersom brottslingarna använder internet både som ett sätt att utöka verksamheten och som en källa för att hitta nya metoder och verktyg för sin brottslighet[6]. I de allra flesta fallen är chanserna att spåra brottslingarna dock minimala, och chanserna att åtala dem ännu mindre.

Samtidigt använder statliga aktörer inte bara traditionella verktyg som militär styrka för att uppnå sina geopolitiska mål, utan använder även mer diskreta cyberverktyg, bland annat genom att ingripa i interna demokratiska processer. Användningen av cyberrymden som en plats för krigsoperationer, antingen ensamt eller som en del av en hybridstrategi, är nu allmänt erkänd. Desinformationskampanjer, falska nyheter och cyberaktiviteter som riktas mot kritisk infrastruktur blir allt vanligare och kräver ett svar. I sitt diskussionsunderlag om det europeiska försvarets framtid[7] betonar kommissionen därför betydelsen av cyberförsvarssamarbete.

Om vi inte betydligt förbättrar vår cybersäkerhet kommer risken att öka i och med den digitala omvandlingen. Tiotals miljarder ”sakernas internet”-enheter förväntas vara anslutna till internet 2020, men cybersäkerheten är ännu ingen prioritering i deras utformning[8]. Om vi misslyckas med att skydda de enheter som kommer att kontrollera våra elnät, bilar, transportnät, fabriker, finanser, sjukhus och hem, kan detta få förödande konsekvenser och enormt skada konsumenternas förtroende för framväxande teknik. Risken för politiskt motiverade angrepp mot civila mål och brister i det militära cyberförsvaret ökar denna risk ännu mer.

---

1 http://www.consilium.europa.eu/sv/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Se t.ex. McAfee & Centre for Strategic and International Studies *Net losses: Estimating the Global Cost of Cybercrime*, 2014.

4 Ransomware är en typ av sabotageprogram som förhindrar eller begränsar användarnas åtkomst till sina system, antingen genom att låsa systemets skärm eller genom att låsa användarnas filer om inte en lösensumma betalas.

5 I maj 2017 drabbade ransomware-angreppet WannaCry över 400 000 datorer i över 150 länder. En månad senare slog ransomware-angreppet Petya till mot Ukraina och företag i hela världen.

6 Europols hotbildsbedömning avseende grov och organiserad brottslighet 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_sv.pdf.

8 *IDC and TXT Solutions* (2014), *SMART 2013/0037 Cloud and IoT combination*, undersökning på uppdrag från kommissionen.

Syftet med den strategi som beskrivs i detta gemensamma meddelande är att göra EU bättre rustat för att bemöta dessa hot. Målen är att bygga upp högre resiliens och strategiskt oberoende, öka den tekniska kapaciteten och förbättra kompetensen samt bidra till att bygga upp en stark inre marknad. För att åstadkomma detta måste de rätta strukturerna finnas på plats så att vi kan bygga upp en stark cybersäkerhet och reagera när det krävs, med fullständigt deltagande av alla viktiga aktörer. Strategin kommer även att bidra till att vi kan avskräcka från cyberangrepp på ett bättre sätt, genom att öka insatserna för att upptäcka, spåra och lagföra de ansvariga. Den omfattar även den globala dimensionen, genom utveckling av internationellt samarbete som en plattform för EU:s ledarskap på cybersäkerhetsområdet. Dessa åtgärder bygger på strategierna för den digitala inre marknaden, den globala strategin, den europeiska säkerhetsagendan[9], den gemensamma ramen för att motverka hybridhot[10] och meddelandet *Start för Europeiska försvarsfonden*[11][12].

EU arbetar redan med många av dessa frågor, och det är nu dags att samla de olika arbetsflödena. År 2013 utarbetade EU en strategi för cybersäkerhet, och i och med detta inleddes en rad arbetsflöden för att förbättra cyberresiliensen[13]. Strategins huvudsakliga mål, att främja ett tillförlitligt, säkert och öppet cyberekosystem, gäller fortfarande. Den ständigt utvecklande och fördjupade hotbilden kräver dock fler åtgärder för att stå emot och avskräcka från angrepp i framtiden[14].

EU är väl lämpat att hantera cybersäkerhet, med tanke på omfattningen av dess politik och de verktyg, strukturer och kapacitet som EU förfogar över. Medlemsstaterna är fortfarande ansvariga för den nationella säkerheten, men omfattningen av och den gränsöverskridande karaktären hos detta hot gör EU-åtgärder väl motiverade. EU kan bidra med incitament och stöd till medlemsstaterna så att de kan utveckla och upprätthålla ökad och bättre nationell kapacitet för cybersäkerhet, samtidigt som kapaciteten byggs upp på EU-nivå. Denna strategi är utformad för att sporra alla aktörer – EU, medlemsstaterna, näringslivet och individer – att prioritera cybersäkerhet på det sätt som krävs för att bygga upp resiliens och förbättra EU:s svarsåtgärder mot cyberangrepp. Strategin kommer att tillföra konkreta åtgärder för att hjälpa till att upptäcka och utreda alla former av cyberangrepp mot EU och dess medlemsstater och agera därefter, bland annat genom att åtala brottslingar. Strategin kommer även bidra till att EU inom sina yttre åtgärder effektivt kan främja cybersäkerhet på den globala arenan. Resultatet kommer att bli att EU går över från en reaktiv till en proaktiv strategi för att skydda EU:s välstånd, samhällen, värderingar och grundläggande fri- och rättigheter, genom att hantera både befintliga och framtida hot.

2. BYGGA UPP EU:S RESILIENS MOT CYBERANGREPP

En stark cyberresiliens kräver ett gemensamt och heltäckande tillvägagångssätt. Detta kräver i sin tur mer robusta och effektiva strukturer för att främja cybersäkerhet och hantera cyberangrepp i medlemsstaterna, men även inom EU:s egna institutioner, byråer och organ. Det krävs dessutom en mer omfattande tvärpolitisk strategi för att bygga upp cyberresiliens

[9] COM(2015) 185 final.
[10] JOIN(2016) 18 final.
[11] COM(2017) 295.
[12] Strategin underbyggs även av oberoende vetenskapliga råd som har lämnats av Europeiska kommissionens mekanism för vetenskaplig rådgivning – högnivågruppen av vetenskapliga rådgivare (se hänvisningar nedan).
[13] JOIN(2013) 1 final. En bedömning av strategin finns i arbetsdokumentet SWD (2017) 295.
[14] Om inte annat anges är förslagen i detta meddelande budgetneutrala. Eventuella initiativ som får budgetkonsekvenser kommer att följa de årliga budgetförfarandena och kan inte påverka nästa fleråriga budgetram efter 2020.

och strategiskt oberoende, med en stark inre marknad, stora framsteg i fråga om EU:s tekniska kapacitet och många fler kompetenta experter. Grunden för detta är ett mer allmänt accepterande av att cybersäkerhet är en gemensam samhällsutmaning, vilket innebär att flera nivåer i styrningen, ekonomin och samhället bör vara involverade.

2.1 Stärka Europeiska unionens byrå för nät- och informationssäkerhet

Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) spelar en central roll för att stärka EU:s cyberresiliens och svarsinsatser, men begränsas av sitt nuvarande mandat. Kommissionen lägger därför fram ett ambitiöst reformförslag, som bland annat innehåller ett **permanent mandat för byrån**[15]. Detta kommer att säkerställa att Enisa kan stödja medlemsstaterna, EU-institutionerna och företagen på viktiga områden, bland annat med genomförandet av direktivet om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen[16] (nedan kallat *direktivet om nät- och informationssäkerhet*), och den föreslagna certifieringsramen för cybersäkerhet.

Det reformerade Enisa kommer att ha en stark rådgivande roll i fråga om utformningen och genomförandet av politiska åtgärder, och kommer bland annat att främja samstämmighet mellan sektorsinitiativ och direktivet om nät- och informationssäkerhet samt bidra till att inrätta informations- och analyscentraler inom kritiska sektorer. Enisa kommer att höja ribban och förbättra EU:s beredskap genom att anordna årliga Europaomfattande cybersäkerhetsövningar som kombinerar svarsåtgärder på olika nivåer. Byrån kommer även att bidra till utvecklingen av EU:s politik för cybersäkerhetscertifiering med hjälp av informations- och kommunikationsteknik (IKT) och spela en viktig roll för att öka både det operativa samarbetet och krishanteringen i EU. Enisa kommer dessutom att fungera som kontaktpunkt för information och kunskap inom cybersäkerhetsbranschen.

En snabb och gemensam förståelse av hot och incidenter allteftersom de utvecklas är en nödvändig förutsättning för beslut om huruvida det krävs gemensamma begränsande åtgärder eller svarsåtgärder på EU-nivå. Ett sådant informationsutbyte kräver deltagande av alla relevanta aktörer – EU:s organ och byråer och medlemsstaterna – på teknisk, operativ och strategisk nivå. I samarbete med relevanta organ på medlemsstats- och EU-nivå, särskilt nätverket av enheter för hantering av it-säkerhetsincidenter (Computer Security Incident Response Teams, CSIRT)[17], Cert-EU, Europol och Europeiska unionens underrättelseanalyscentrum (Intcen), kommer Enisa också att bidra till situationsmedvetenhet på EU-nivå. Detta kan i sin tur bidra till analys av hotbilder och beslutsfattande inom ramen för regelbunden övervakning av hotbilden samt effektivt operativt samarbete, och kan även vara till hjälp för att hantera storskaliga gränsöverskridande incidenter.

2.2 Mot en inre cybersäkerhetsmarknad

Cybersäkerhetsmarknadens tillväxt i EU, både när det gäller produkter, tjänster och processer, hämmas på flera olika sätt. En viktig aspekt är att det saknas certifieringssystem för cybersäkerhet som erkänns i hela EU för att bygga in högre nivåer av resiliens i produkterna och förbättra marknadens förtroende i EU. Kommissionen lägger därför fram ett förslag om inrättandet av en **certifieringsram för cybersäkerhet på EU-nivå**[18]. Ramen är tänkt att utgöra grunden för ett förfarande för att skapa EU-omfattande certifieringssystem för

[15] COM(2017) 477.

[16] Europaparlamentets och rådets direktiv 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

[17] Enligt artikel 9 i direktivet om nät- och informationssäkerhet.

[18] COM(2017) 477.

cybersäkerhet, vilket skulle omfatta produkter, tjänster och/eller system och anpassa konfidensgraden till det berörda användningsområdet (vare sig det rör sig om kritiska infrastrukturer eller konsumentenheter)[19]. Ett sådant certifieringssystem skulle ge tydliga fördelar för företagen, eftersom de inte behöver gå igenom flera certifieringsprocesser när de bedriver gränsöverskridande verksamhet, och på så sätt kan minska sina administrativa och ekonomiska kostnader. Användningen av system som utvecklats inom denna ram skulle också bidra till att bygga upp konsumenternas förtroende med ett intyg om överensstämmelse som informerar och lugnar köpare och användare i fråga om säkerhetsegenskaperna hos de produkter och tjänster som de köper och använder. På så sätt skulle höga cybersäkerhetsstandarder bli en konkurrensfördel. Resultatet skulle bli ökad resiliens, eftersom IKT-produkter och IKT-tjänster formellt utvärderas mot en fastställd uppsättning cybersäkerhetsstandarder, som skulle utformas i nära anslutning till det mer allmänna pågående arbetet med IKT-standarder[20].

Ramens system skulle vara frivilliga och skulle inte ge upphov till några omedelbara lagstadgade skyldigheter för produkt- eller tjänsteleverantörer. Systemen skulle inte heller strida mot tillämpliga rättsliga krav, t.ex. EU-lagstiftningen om uppgiftsskydd.

När ramen har inrättats kommer kommissionen att uppmana relevanta intressenter att inrikta sig på tre prioritetsområden:

- Säkerhet i kritiska tillämpningar eller tillämpningar med hög risk[21]: system som vi är beroende av i våra dagliga aktiviteter, från bilar till maskiner i fabriker, från de största systemen som flygplan eller kraftverk till de minsta som medicintekniska produkter, blir alltmer digitala och sammankopplade. Centrala IKT-komponenter i sådana produkter och system kräver därför noggranna säkerhetsbedömningar.

- Cybersäkerhet i vanliga digitala produkter, nät, system och tjänster som används både inom den privata och den offentliga sektorn för att bygga upp ett försvar mot angrepp och tillämpa lagstadgade skyldigheter[22] – såsom e-postkryptering, brandväggar och virtuella privata nät: här är det viktigt att den alltmer spridda användningen av sådana verktyg inte leder till nya riskkällor eller sårbarheter.

- Användningen av metoder för ”inbyggd säkerhet” i billiga digitala sammankopplade masskonsumentenheter som tillsammans bildar sakernas internet: ramens system skulle användas för att ange att produkterna byggs med toppmoderna och säkra utvecklingsmetoder, att de har genomgått lämplig säkerhetstestning och att säljarna har åtagit sig att uppdatera sin programvara i händelse av nyupptäckta sårbarheter eller hot.

Särskilt viktiga aspekter i prioriteringarna skulle vara den utvecklande hotbilden för cybersäkerhet och vikten av grundläggande tjänster som transport, energi, hälsovård, banker, finansmarknadsinfrastrukturer, dricksvatten eller digital infrastruktur[23].

---

[19] En konfidensgrad anger hur sträng säkerhetsbedömningen är och motsvarar vanligen den risknivå som är förknippad med tillämpningens användningsområde eller funktioner (det krävs t.ex. en högre konfidensgrad för IKT-produkter eller IKT-tjänster som används i tillämpningar eller funktioner med hög risk).

[20] COM(2016) 176.

[21] Undantaget är om obligatorisk eller frivillig certifiering styrs av andra unionsakter.

[22] Direktiv (EU) 2016/1148, förordning (EU) 2016/679, direktiv (EU) 2015/2366 och andra lagstiftningsförslag, såsom den europeiska koden för elektronisk kommunikation, kräver t.ex. att organisationer inför lämpliga säkerhetsåtgärder för att hantera relevanta cybersäkerhetsrisker.

[23] De sektorer som omfattas av Europaparlamentets och rådets direktiv 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Det är omöjligt att garantera att IKT-produkter, IKT-system eller IKT-tjänster är ”100 %” säkra, men det finns flera välkända och väldokumenterade defekter i utformningen av IKT-produkter som kan utnyttjas för angrepp. Om producenter av anslutna enheter, it-programvara och it-utrustning tillämpar inbyggd säkerhet skulle det vara möjligt att garantera att cybersäkerhetsaspekterna hanteras innan nya produkter släpps ut på marknaden. Detta skulle kunna ingå i principen om aktsamhetsplikt, som skulle utvecklas i samarbete med branschen och bidra till att minska produkternas/programvarans sårbarheter genom tillämpning av en rad metoder, från utformning till testning och kontroll, även formell kontroll i tillämpliga fall, långsiktigt underhåll och användning av säkra utvecklingsprocesser för produkternas livscykel, och även bidra till att utveckla uppdateringar och programfixar för att hantera tidigare oupptäckta sårbarheter och för snabb uppdatering och reparation[24]. Det skulle också bidra till att öka konsumenternas förtroende för digitala produkter.

Den viktiga roll som utomstående säkerhetsforskare spelar för att upptäcka sårbarheter hos befintliga produkter och tjänster måste också erkännas, och förutsättningar bör skapas för att möjliggöra samordnad information om sårbarheter[25] i medlemsstaterna genom att bygga på bästa praxis[26] och relevanta standarder[27].

Samtidigt har **specifika sektorer** särskilda problem, och bör uppmuntras att utforma sina egna strategier. På så sätt skulle de allmänna cybersäkerhetsstrategierna kompletteras med specifika cybersäkerhetsstrategier inom områden som finansiella tjänster[28], energi, transport och hälsa[29].

Kommissionen har redan lyft fram de särskilda **ansvarsrelaterade** problem som har uppkommit i och med de nya digitala teknikerna[30] och arbetar med att analysera följderna. Arbetet med kommande åtgärder kommer att avslutas i juni 2018. Cybersäkerhet ger upphov till problem i samband med fastställande av skada för företag och leverantörskedjor. Dessa problem måste lösas, eftersom de annars kommer att hindra utvecklingen av en stark inre marknad för produkter och tjänster på cybersäkerhetsområdet.

Utvecklingen av en inre EU-marknad är även beroende av att cybersäkerhet integreras i handels- och investeringspolitiken. Effekten av utländska förvärv på kritiska tekniker – som cybersäkerhet är ett viktigt exempel på – är en central aspekt inom ramen för **kontrollen av utländska direktinvesteringar i Europeiska unionen**[31], som syftar till att möjliggöra kontroll av investeringar från tredjeländer av hänsyn till allmän ordning och säkerhet. På samma sätt har cybersäkerhetskrav redan gett upphov till handelshinder för varor och tjänster från EU inom viktiga sektorer i ett antal tredjelandsekonomier. EU:s certifieringsram för cybersäkerhet kommer att ytterligare stärka Europas internationella ställning, och bör

---

[24] Cybersäkerhet på EU:s digitala inre marknad, högnivågruppen av vetenskapliga rådgivare, mars 2017

[25] Samordnad information om sårbarheter är en samarbetsform som underlättar och gör det möjligt för säkerhetsforskare att rapportera sårbarheter till informationssystemets ägare eller säljare, så att organisationen snabbt kan diagnostisera och avhjälpa svagheten på ett lämpligt sätt innan detaljerad information om den berörda svagheten lämnas ut till tredje part eller allmänheten.

[26] Till exempel *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*, Enisa, 2016.

[27] ISO/IEC 29147:2014 *Information technology -- Security techniques -- Vulnerability disclosure*.

[28] Kommissionens kommande arbete med finansteknik kommer att omfatta cybersäkerhet för finanssektorn.

[29] Till exempel inom energisektorn, genom att kombinera mycket gammal teknik med spetsteknik, särskilt realtidskrav för elnätet.

[30] COM(2017) 228.

[31] COM(2017) 478.

kompletteras med fortsatta ansträngningar mot utvecklingen av globala standarder med hög säkerhet och överenskommelser om ömsesidigt erkännande.

2.3 Fullständigt genomförande av direktivet om nät- och informationssäkerhet

De viktigaste verktygen för att bekämpa cybersäkerhetsincidenter finns i dag på nationell nivå, men EU har bekräftat behovet av att verka för högre standarder. Storskaliga cybersäkerhetsincidenter drabbar sällan bara en medlemsstat till följd av den alltmer globaliserade, digitalberoende och sammankopplade karaktären hos centrala sektorer som bank-, energi- eller transportsektorn.

Direktivet om nät- och informationssäkerhet är den första EU-omfattande rättsakten om cybersäkerhet[32]. Det är utformat för att bygga upp resiliensen genom att förbättra den nationella cybersäkerhetskapaciteten, främja bättre samarbete mellan medlemsstaterna och kräva att företag inom viktiga ekonomiska sektorer inför effektiva riskhanteringsmetoder och rapporterar allvarliga incidenter till de nationella myndigheterna. Dessa skyldigheter gäller även tre typer av leverantörer av viktiga internettjänster: molntjänster, sökmotorer och internetbaserade marknadsplatser. Syftet är att skapa en starkare och mer systematisk strategi och ett bättre informationsflöde.

Medlemsstaterna ska genomföra direktivet till maj 2018, vilket är mycket viktigt för EU:s cyberresiliens. Medlemsstaterna arbetar gemensamt för att stödja processen, och riktlinjer kommer till hösten 2017 för att stödja ett mer harmoniserat genomförande, särskilt när det gäller operatörer av grundläggande tjänster. Kommissionen utfärdar även ett meddelande[33] som en del av cybersäkerhetspaketet för att stödja dessa insatser genom att tillhandahålla bästa praxis från medlemsstaterna om direktivets genomförande och vägledning om hur direktivet bör fungera i praktiken.

Ett område där direktivet behöver kompletteras är informationsflödet. Direktivet omfattar t.ex. endast tre viktiga strategiska sektorer, men logiskt sett är det nödvändigt att alla intressenter som drabbas av cyberangrepp tillämpar ett liknande tillvägagångssätt för att det ska vara möjligt att göra en systematisk bedömning av sårbarheter och ingångspunkter för cyberangripare. Dessutom finns ett antal hinder för samarbetet och informationsutbytet mellan den offentliga och den privata sektorn. Regeringar och offentliga myndigheter är ovilliga att dela med sig av relevant information om cybersäkerhet i rädsla för att äventyra den nationella säkerheten eller konkurrenskraften. Privata företag är å sin sida motvilliga att dela med sig av information om sina cybersårbarheter och resulterande förluster av rädsla för att äventyra känslig affärsinformation, riskera sitt anseende eller riskera att bryta mot uppgiftsskyddsregler[34]. Förtroendet för offentlig-privata partnerskap måste förbättras för att underbygga ett bredare samarbete och informationsutbyte mellan fler sektorer. Informations- och analyscentralerna spelar en särskilt viktig roll för att skapa det nödvändiga förtroendet för informationsutbyte mellan den privata och den offentliga sektorn. Vissa inledande åtgärder har redan vidtagits i fråga om särskilt kritiska sektorer, t.ex. inom luftfarten genom inrättandet

[32] Europaparlamentets och rådets direktiv 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

[33] COM(2017) 476.

[34] Cybersäkerhet på EU:s digitala inre marknad, högnivågruppen av vetenskapliga rådgivare, mars 2017. Företagshemligheter är ett särskilt problem i detta sammanhang, och kommissionen konstaterar i sitt meddelande *Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch* från juli 2016 att det finns en ovilja att rapportera cyberstöld av företagshemligheter och att tillförlitliga rapporteringskanaler som garanterar konfidentialitet därför är viktiga.

av det europeiska centrumet för it-säkerhet inom luftfart,[35] och inom energisektorn, genom att inrätta informations- och analyscentraler[36]. Kommissionen kommer att engagera sig helhjärtat i denna strategi med stöd från Enisa, för att se till att utvecklingen påskyndas i sektorer som tillhandahåller grundläggande tjänster enligt direktivet om nät- och informationssäkerhet.

2.4 Resiliens genom snabb incidenthantering

Vid cyberangrepp kan snabba och effektiva svarsåtgärder begränsa följderna. Det kan också visa att de offentliga myndigheterna inte står maktlösa inför cyberangrepp, och därmed bidra till att bygga upp förtroendet. När det gäller EU-institutionernas egna svarsåtgärder bör cyberaspekter i första hand integreras i EU:s befintliga krishanteringsmekanismer: EU-arrangemang för integrerad politisk krishantering, som samordnas av rådets ordförandeskap,[37] och EU:s allmänna system för snabb varning[38]. Behovet av att hantera särskilt allvarliga cyberincidenter eller angrepp bör vara en tillräcklig grund för medlemsstaterna att åberopa EU:s solidaritetsklausul[39].

Snabba och effektiva svarsåtgärder är även beroende av att det finns en mekanism för snabbt informationsutbyte mellan alla centrala aktörer på EU-nivå, vilket i sin tur kräver en tydlig fördelning av deras respektive roller och ansvar. Kommissionen har rådfrågat EU-institutionerna och medlemsstaterna om en konkret plan för att skapa en effektiv process på unions- och medlemsstatsnivå för operativa svarsåtgärder vid storskaliga cyberincidenter. I den **konkreta plan** som läggs fram i en rekommendation[40] som ingår i detta paket förklaras hur cybersäkerhet integreras i de befintliga krishanteringsmekanismerna på EU-nivå. Planen anger även mål och samarbetsmetoder mellan medlemsstaterna och mellan dem och relevanta institutioner, avdelningar, byråer och organ på EU-nivå[41] när det gäller hanteringen av storskaliga cybersäkerhetsincidenter och kriser. I rekommendationen uppmanas även medlemsstaterna och EU-institutionerna att inrätta en krishanteringsram för cybersäkerhet i EU för att omsätta den konkreta planen i praktiken. Den konkreta planen kommer att testas regelbundet vid cybersäkerhetsrelaterade och andra krishanteringsövningar[42] och uppdateras vid behov.

Med tanke på att cybersäkerhetsincidenter kan få allvarliga återverkningar på ekonomiernas funktion och människors vardag skulle ett alternativ kunna vara att undersöka möjligheten att inrätta en **fond för hantering av cybersäkerhetsincidenter**, i linje med andra sådana krismekanismer inom andra EU-politikområden. På så sätt skulle medlemsstaterna kunna söka hjälp på EU-nivå under eller efter en allvarlig incident, förutsatt att de har infört ett lämpligt cybersäkerhetssystem före incidenten och fullständigt har genomfört direktivet om nät- och informationssäkerhet samt har väletablerade riskhanterings- och övervakningssystem på nationell nivå. En sådan fond, som skulle komplettera befintliga krishanteringsmekanismer på

---

35 https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

36 Det rör sig om ideella och medlemsbaserade organisationer som bildas av privata och offentliga enheter för att utbyta information om cyberhot, risker, förebyggande, begränsande åtgärder och svarsåtgärder. Se t.ex. European Energy Information Sharing and Analysis Centres (http://www.ee-isac.eu).

37 Detta möjliggör samordning av svarsåtgärder vid stora sektorsöverskridande kriser på högsta politiska nivå.

38 Detta möjliggör internt informationsutbyte och samordning om framväxande kriser som omfattar flera sektorer, eller förutsebara eller överhängande hot som kräver åtgärder på EU-nivå.

39 Enligt artikel 222 i fördraget om Europeiska unionens funktionssätt.

40 C(2017) 6100.

41 Inklusive Europol, Enisa, organisationen för incidenthantering som ansvarar för säkerheten i it-systemen hos EU:s institutioner, byråer och organ (Cert-EU) och Europeiska unionens underrättelseanalyscentrum (Intcen).

42 Till exempel de som genomförs av Enisa: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

EU-nivå, kan tillhandahålla kapacitet för snabba svarsåtgärder i solidaritetens intresse och finansiera specifika krishanteringsåtgärder, t.ex. ersätta äventyrad utrustning eller använda begränsnings- eller svarsverktyg genom att bygga på nationell sakkunskap i linje med EU:s civilskyddsmekanism.

2.5 Ett nätverk för cybersäkerhetskompetens med ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet

Cybersäkerhetstekniska verktyg är strategiska tillgångar, samtidigt som de är viktiga tillväxttekniker inför framtiden. Det ligger i EU:s strategiska intresse att se till att EU behåller och utvecklar grundläggande kapacitet för att trygga den digitala ekonomin, samhället och demokratin, skyddar kritisk maskin- och programvara och tillhandahåller viktiga cybersäkerhetstjänster.

Det offentlig-privata partnerskap om cybersäkerhet[43] som skapades 2016 var ett viktigt första steg, och kommer att ge upp till 1,8 miljarder euro i investeringar fram till 2020. Omfattningen av de investeringar som görs i andra delar av världen[44] visar dock att EU måste mobilisera mer investeringar och lösa problemet med splittrad kapacitet i EU.

EU kan bidra med mervärde med tanke på sin avancerade cybersäkerhetsteknik, de storskaliga investeringar som krävs och behovet av lösningar som fungerar i hela EU. Genom att bygga vidare på medlemsstaternas och det offentlig-privata partnerskapets arbete är nästa steg att förstärka EU:s cybersäkerhetskapacitet genom ett **nätverk för cybersäkerhetskompetenscentrum**[45] med ett **europeiskt forsknings- och kompetenscentrum för cybersäkerhet** som grund. Nätverket och centrumet skulle stimulera utveckling och införande av cybersäkerhetsteknik och komplettera insatserna för att bygga upp kapaciteten inom detta område på EU-nivå och nationell nivå. Kommissionen kommer att inleda en konsekvensbedömning för att undersöka tillgängliga alternativ, även möjligheten att inrätta ett gemensamt företag, med målet att införa denna struktur 2018.

Som ett första steg och som underlag för framtida diskussioner kommer kommissionen att föreslå att en pilotfas inleds inom ramen för Horisont 2020, för att sammanföra de nationella centrumen i ett nätverk som skapar ny drivkraft för cybersäkerhetskompetens och teknisk utveckling. Kommissionen planerar att föreslå en kortsiktig finansiering på 50 miljoner euro för detta ändamål. Denna verksamhet kommer att komplettera det pågående genomförandet av det offentlig-privata partnerskapet om cybersäkerhet.

Nätverkets huvudsakliga syfte och centrumets inledande mål skulle vara att sammanföra och utforma forskningsinsatser. För att stödja utvecklingen av industriell kapacitet skulle centrumet agera som projektledare för kapacitetsskapande och hantera multinationella projekt. Detta skulle även ge extra drivkraft för EU-industrins innovationsförmåga och konkurrenskraft på den globala arenan när det gäller utveckling av nästa generations digitala tekniker, inbegripet artificiell intelligens, kvantdatateknik, blockkedjeteknik och säkra digitala identiteter samt säkrad åtkomst till massdata för EU-baserade företag, vilka alla är avgörande för framtidens cybersäkerhet. Centrumet skulle även bygga vidare på EU:s arbete med att utöka infrastrukturen för högpresterande datorsystem: detta är avgörande för analys av stora

[43] C(2016) 4400 final.

[44] USA kommer att investera 19 miljarder US-dollar bara under 2017, en ökning på 35 % jämfört med 2016. Vita huset, pressekreterarens kontor: ‘Faktablad: Cybersecurity National Action Plan’, 9 februari 2016.

[45] Nätverket skulle omfatta befintliga och framtida cybersäkerhetscentrum som inrättas i medlemsstaterna, vars medlemmar främst utgörs av offentliga forskningsorganisationer och laboratorier.

datamängder, snabb kryptering och dekryptering av data, identitetskontroller, simulerade cyberangrepp och analys av videomaterial[46].

Nätverket av kompetenscentrum skulle även kunna ha kapacitet att stödja industrin genom testning och simuleringar för att stödja den cybersäkerhetscertifiering som beskrivs i avsnitt 2.2. Nätverkets deltagande i EU:s övergripande arbete på cybersäkerhetsområdet skulle å sin sida säkerställa en kontinuerlig uppdatering av arbetets inriktning efter behov. Centrumets mål skulle vara att verka för höga cybersäkerhetsstandarder, inte bara i teknik- och cybersäkerhetssystem, utan även när det gäller utveckling av avancerad kompetens för yrkesverksamma, genom att tillhandahålla lösningar och modeller för nationella insatser för digital kompetens. Centrumet skulle även stärka cybersäkerhetskapaciteten på EU-nivå och utnyttja synergier, särskilt med Enisa, Cert-EU, Europol, den eventuella framtida fonden för hantering av cybersäkerhetsincidenter och nationella CSIRT.

Ett prioriterat arbetsområde för kompetensnätverket måste vara den bristande europeiska kapaciteten att bedöma **kryptering** av produkter och tjänster som används av allmänheten, företag och regeringar på den inre digitala marknaden. Stark kryptering är grunden för säkra digitala identifieringssystem, som spelar en avgörande roll för en effektiv cybersäkerhet[47]. Kryptering skapar också säkerhet för personers immateriella tillgångar och gör det möjligt att skydda grundläggande rättigheter som yttrandefrihet och skydd av personuppgifter, samtidigt som den garanterar säker e-handel[48].

EU:s marknader för civil- och försvarsrelaterad cybersäkerhet har gemensamma utmaningar[49] och teknik med dubbla användningsområden som kräver nära samarbete på kritiska områden. Därför skulle nätverket och dess centrum kunna utvecklas i en andra fas med en cyberförsvarsdimension, med fullständig respekt för fördragsbestämmelserna om den gemensamma säkerhets- och försvarspolitiken. Precis som den tekniska inriktningen skulle försvarsdimensionen kunna bidra till samarbete mellan medlemsstaterna på cyberförsvarsområdet, bland annat genom informationsutbyte, situationsmedvetenhet, skapande av sakkunskap och samordnade åtgärder, med stöd till medlemsstaternas utveckling av gemensam kapacitet. Centrumet skulle även fungera som en plattform där medlemsstaterna kan enas om prioriteringar för EU:s cyberförsvar, undersöka gemensamma lösningar, bidra till utvecklingen av gemensamma strategier, underlätta gemensam utbildning, övningar och testning på cyberförsvarsområdet på EU-nivå, och stödja arbetet med klassificering och standarder om cyberförsvar, där centrumet skulle ha en stödjande och rådgivande roll. För att kunna utföra dessa uppgifter måste centrumet arbeta nära med och fullständigt anpassa sig till Europeiska försvarsbyrån på cybersäkerhetsområdet samt med Enisa när det gäller cyberresiliens. Den process som inleddes i och med diskussionsunderlaget om det europeiska försvarets framtid skulle fullständigt beaktas i denna försvarsdimension.

Den höga resiliens som krävs för cyberförsvar kräver riktade forsknings- och teknikinsatser. Projekt eller tekniker för cyberförsvar som utvecklas av företag skulle kunna få finansiering från Europeiska försvarsfonden, både i forsknings- och utvecklingsfasen[50]. Vissa områden kan vara särskilt relevanta i detta sammanhang, såsom krypteringssystem som baseras på kvanttekniker, situationsmedvetenhet på cyberområdet, kontrollsystem för biometrisk

[46] COM(2012) 45 final och COM(2016) 178 final.

[47] Inom ramen för Horisont 2020 kommer kommissionen att inrätta ett nytt Horisontpris på 4 miljoner euro för den bästa innovativa lösningen för sömlösa e-autentiseringsmetoder..

[48] Cybersäkerhet på EU:s digitala inre marknad, högnivågruppen av vetenskapliga rådgivare, mars 2017.

[49] *Study on synergies between the civilian and the defence cybersecurity markets* (Optimity; Smart 2014-0059).

[50] Den europeiska försvarsindustrins utvecklingsprogram kommer redan nu att prioritera cyberförsvarsprojekt, och cyberförsvar kommer att vara ett av ämnena i den ansökningsomgång som kommer att inledas 2018.

åtkomst, upptäckt av avancerade långvariga hot eller datautvinning. Utrikesrepresentanten, Europeiska försvarsbyrån och kommissionen kommer att hjälpa medlemsstaterna att identifiera områden där gemensamma cybersäkerhetsprojekt kan övervägas för finansiering från Europeiska försvarsfonden.

2.6 Bygga upp en stark cyberkompetensbas i EU

Cybersäkerhet har en stark utbildningsdimension. Effektiv cybersäkerhet är starkt beroende av de berörda personernas kompetens. Kompetensunderskottet när det gäller yrkesverksamma på cybersäkerhetsområdet i den privata sektorn i Europa beräknas dock uppgå till 350 000 till 2022[51]. Utbildning i cybersäkerhet bör därför utvecklas på alla nivåer, från regelbunden utbildning av cyberarbetskraften, kompletterande cybersäkerhetsutbildning för alla IKT-specialister till nya, särskilda kursplaner för cybersäkerhet. Starka akademiska kompetenscentrum bör inrättas för att tillgodose det ökande behovet av allmän och yrkesinriktad utbildning, som kan vägledas av riktlinjer från ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet och Enisa. Målet bör vara att det blir naturligt att utforma IKT-produkter och IKT-system med inbyggda säkerhetsprinciper ända från början. Cybersäkerhetsutbildningen bör inte endast begränsas till it-personal, utan bör integreras i kursplanerna för andra områden, t.ex. teknik, affärsledning eller juridik samt i sektorsspecifika utbildningar. Lärare och elever i grund- och gymnasieskolan bör också göras medvetna om cybersäkerhet inom ramen för förvärvandet av digital kompetens i skolan.

Tillsammans med medlemsstaterna bör även EU bidra till detta genom att bygga vidare på arbetet inom ramen för koalitionen för digital kompetens och digitala arbetstillfällen[52] och genom att t.ex. införa praktiksystem för små och medelstora företag på cybersäkerhetsområdet.

2.7 Främja it-hygien och cybermedvetande

Cirka 95 % av incidenterna anses uppstå till följd av ”någon typ av mänskligt fel – avsiktligt eller ej”,[53] vilket innebär det finns en stark mänsklig faktor. Cybersäkerhet är alltså allas ansvar. Detta kräver en beteendeförändring, både på det personliga planet och bland företag och offentliga förvaltningar, för att se till att alla förstår hoten och har tillgång till de verktyg och färdigheter som krävs för att snabbt upptäcka och aktivt skydda sig mot angrepp. Människorna behöver utveckla sunda it-vanor och företag och organisationer måste införa lämpliga riskbaserade cybersäkerhetsprogram och uppdatera dem regelbundet för att avspegla den utvecklande riskbilden.

Enligt direktivet om nät- och informationssäkerhet har medlemsstaterna ansvar för att utbyta information om cyberangrepp på EU-nivå, men de ska också införa mogna nationella cybersäkerhetsstrategier och ramar för säkerheten hos nätverks- och informationssystem. Offentliga förvaltningar på EU-nivå och nationell nivå bör spela en ledarroll och driva på dessa insatser.

För det första bör medlemsstaterna maximera tillgången till cybersäkerhetsverktyg för företag och individer. Mer behöver särskilt göras för att förebygga och begränsa cyberbrottslighetens effekter på slutanvändarna. Ett exempel finns redan, nämligen Europols arbete med kampanjen ”NoMoreRansom”[54], som har tagits fram genom nära samarbete mellan

[51] *Global Information Security Workforce Study 2017*. Den totala bristen uppgår till 1,8 miljoner.
[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.
[53] IBM, *The Cybersecurity Intelligence Index*, 2014, som nämns på Securitymagazine.com, 19 juni 2014.
[54] https://www.nomoreransom.org/.

brottsbekämpande myndigheter och cybersäkerhetsföretag för att hjälpa användarna att förhindra ransomware-infektioner och dekryptera data om de faller offer för en sådan attack. Sådana system bör även införas för andra typer av sabotageprogram och inom andra områden, och EU bör utforma en **gemensam portal för att sammanföra alla sådana verktyg i en samservice,** som erbjuder rådgivning till användarna om förebyggande och upptäckt av sabotageprogramvara och innehåller länkar till rapporteringsmekanismer.

För det andra bör medlemsstaterna påskynda **användningen av mer cybersäkra verktyg i utvecklingen av e-förvaltning**, och även fullständigt utnyttja kompetensnätverket. Införandet av säkra identifieringsmetoder bör främjas, vilket bör bygga på EU:s ram för elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden, som har varit i kraft sedan 2016 och innehåller förutsägbara regler för att möjliggöra säkra och sömlösa elektroniska kontakter mellan företag, individer och offentliga myndigheter[55]. Offentliga institutioner, särskilt sådana som tillhandahåller grundläggande tjänster, bör dessutom se till att deras personal får utbildning på cybersäkerhetsrelaterade områden.

För det tredje bör medlemsstaterna prioritera cybermedvetenhet i **informationskampanjer**, även kampanjer som riktas mot skolor, universitet, näringslivet och forskningsorgan. Cybersäkerhetsmånaden, som hålls varje år i oktober under samordning av Enisa, kommer att utökas för att bredda dess räckvidd som en gemensam kommunikationsinsats på EU-nivå och nationell nivå. Insatser för ökat medvetande i samband med **desinformationskampanjer och falska nyheter** på sociala medier som är särskilt avsedda att undergräva demokratiska processer och europeiska värderingar är lika viktiga. Det primära ansvaret ligger fortfarande på nationell nivå, även i fråga om valet till Europaparlamentet, men sammanförande av sakkunskap och erfarenhetsutbyte på EU-nivå har visat sig tillföra mervärde i form av riktade insatser[56].

Även **industrin** har en stark roll att spela generellt, men med särskild uppmärksamhet på leverantörer och tillverkare av digitala tjänster. Industrin måste stödja användarna (individer, företag och offentliga förvaltningar) med verktyg som gör att de kan ta ansvar för sitt agerande på nätet, och klargöra att sunda it-vanor är en oumbärlig del av konsumentutbudet[57]. För att upptäcka och undanröja sårbarheter bör industrin sträva efter att ha interna processer för utredning, prioritering och lösning av sårbarheter, oberoende om källan till den eventuella sårbarheten var extern eller fanns internt i det berörda företaget.

Viktiga åtgärder

- Fullständigt genomförande av direktivet om nät- och informationssäkerhet.
- Snabbt antagande av Europaparlamentet och rådet av förordningen om ett nytt mandat för Enisa och en europeisk certifieringsram[58].
- Ett gemensamt initiativ mellan kommissionen och industrin för att fastställa en aktsamhetsplikt med målet att minska sårbarheterna hos produkter/programvara och

[55] Förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, antagen den 23 juli 2014. Kommissionen tillhandahåller även hjälpmedel och verktyg för interoperabilitet för e-identifiering och e-signaturer (t.ex. förteckningar över betrodda tjänsteleverantörer) via Fonden för ett sammanlänkat Europa.

[56] Ett exempel är East StratCom Task Force, som inrättades 2015 av medlemsstaterna och utrikesrepresentanten för att hantera Rysslands pågående desinformationskampanjer. Gruppen arbetar med att utveckla kommunikationsprodukter och kampanjer som inriktas på att förklara EU:s politik i den östra partnerskapsregionen.

[57] En del företagare är redan bekanta med detta begrepp, eftersom vissa delar av EU:s produktlagstiftning (t.ex. maskindirektivet 2006/42/EG) föreskriver principer för inbyggd säkerhet.

[58] COM(2017) 477.

främja inbyggd säkerhet.
- Snabbt genomförande av den konkreta planen för gränsöverskridande svarsåtgärder vid allvarliga incidenter.
- Konsekvensbedömning för att undersöka möjligheten till ett kommissionsförslag 2018 om inrättandet av ett nätverk av kompetenscentrum och ett europeiskt forsknings- och kompetenscentrum för cybersäkerhet, som bygger på en pilotfas som inleds omedelbart.
- Stöd till medlemsstaterna så att de kan identifiera områden där gemensamma cybersäkerhetsprojekt kan övervägas för stöd från Europeiska försvarsfonden.
- En EU-omfattande samservice för att hjälpa offer för cyberangrepp, informera om de senaste hoten och samla praktiska råd och cybersäkerhetsverktyg.
- Åtgärder från medlemsstaterna för att integrera cybersäkerhet i kompetensprogram, e-förvaltning och informationskampanjer.
- Åtgärder från industrin för att utöka den cybersäkerhetsrelaterad utbildningen för sin personal och införa en strategi för inbyggd säkerhet för sina produkter, tjänster och processer.

3. SKAPA EFFEKTIVA AVSKRÄCKNINGSMEDEL MOT CYBERBROTT

Effektiva avskräckande åtgärder innebär att införa en ram med åtgärder som både är trovärdiga och avskräckande för eventuella cyberbrottslingar och cyberangripare. Så länge förövarna av cyberangrepp, både statliga och icke-statliga, inte har något att frukta förutom att misslyckas, är det inte mycket som kan få dem att sluta försöka. Effektivare brottsbekämpande åtgärder som inriktas på upptäckt, spårbarhet och åtal av cyberbrottslingar är därför absolut nödvändigt för att bygga upp effektiva avskräckande medel. Förutom detta måste EU hjälpa medlemsstaterna att utveckla cybersäkerhetskapacitet med dubbla användningsområden. För att kunna vända på cyberangreppstrenden måste vi bli bättre på att få tag på cyberbrottslingarna och straffa cyberbrott. Cyberangrepp bör utredas snabbt och förövarna bör ställas inför rätta eller åtgärder vidtas för att möjliggöra ett lämpligt politiskt eller diplomatiskt svar. I händelse av en allvarlig kris med en omfattande internationell och försvarsmässig dimension kan utrikesrepresentanten föreslå rådet alternativ till lämpliga svarsåtgärder.

Ett steg mot att förbättra de straffrättsliga åtgärderna till svar på cyberangrepp togs redan i och med antagandet 2013 av direktivet om angrepp mot informationssystem[59]. Genom direktivet fastställs minimiregler om fastställande av brottsrekvisit och påföljder vad gäller angrepp mot informationssystem och operativa åtgärder för att förbättra samarbetet mellan myndigheterna. Direktivet har lett till avsevärda framsteg med att kriminalisera cyberangrepp på ett jämförbart sätt i medlemsstaterna, vilket underlättar gränsöverskridande samarbete mellan de brottsbekämpande myndigheter som utreder denna typ av brott. Direktivet skulle dock vara ännu effektivare om medlemsstaterna genomförde alla bestämmelser fullt ut[60]. Kommissionen kommer att fortsätta att hjälpa medlemsstaterna i deras genomförande av direktivet och ser för närvarande inget behov av att föreslå ändringar av det.

3.1 Identifiera skadliga aktörer

För att öka chanserna att ställa förövarna inför rätta måste vi snabbt förbättra vår kapacitet att identifiera de personer som är ansvariga för cyberangrepp. Ett stort problem för de

[59] Europaparlamentets och rådets direktiv 2013/40/EG av den 12 augusti 2013 om angrepp mot informationssystem.
[60] COM(2017) 474.

brottsbekämpande myndigheterna är att hitta användbar information för utredningar av cyberbrott, främst i form av digitala spår. Vi måste därför förbättra vår tekniska kapacitet för effektiva utredningar, bland annat genom att förstärka Europols cyberbrottsenhet med cyberexperter. Europol har blivit en viktig aktör för att stödja medlemsstaternas utredningar som sträcker sig över flera jurisdiktioner. Europol bör bli ett expertcentrum för medlemsstaternas brottsbekämpande myndigheter när det gäller internetutredningar och kriminaltekniker som arbetar med cyberbrott.

Den utbredda metoden att placera många användare, ibland tusentals, bakom en IP-adress gör det tekniskt svårt att utreda skadligt beteende på internet. Det leder också till att det ibland blir nödvändigt, t.ex. vid grova brott som sexuella övergrepp mot barn, att utreda många användare för att identifiera en skadlig aktör. EU kommer därför att uppmuntra användning av det nya protokollet (IPv6), eftersom det gör det möjligt att anslå en IP-adress per användare, vilket ger klara fördelar för brotts- och cybersäkerhetsutredningar. Som ett första steg för att uppmuntra användning av protokollet kommer kommissionen att integrera kravet att gå över till IPv6 i sina politiska åtgärder, bland annat i offentliga upphandlingar och i projekt- och forskningsfinansiering. Kommissionen kommer även att bistå med hjälp med nödvändigt utbildningsmaterial. Medlemsstaterna bör dessutom överväga frivilliga avtal med internetleverantörer för att främja användningen av IPv6.

Belgien är ledande i världen[61] *när det gäller införande av IPv6, bl.a. tack vare offentligt-privat samarbete. Relevanta intressenter har övervägt att begränsa användningen av IP-adresser till högst 16 användare som en del av en frivillig självregleringsåtgärd, vilket stimulerade övergången till IPv6*[62].

Mer allmänt bör redovisningsskyldighet på internet främjas. Detta innebär främjande av åtgärder för att förhindra missbruk av domännamn för distribution av oönskade meddelanden eller nätfiske. I detta syfte kommer kommissionen att arbeta för att se till att domännamnssystemet och IP WHOIS-systemet[63] fungerar bättre och att informationen är mer tillgänglig och exakt i linje med de insatser som görs av Internet Corporation for Assigned Names and Numbers[64].

3.2 Skärpa brottsbekämpande svarsåtgärder

Effektiv **utredning** och **lagföring** av cyberbrott är en viktig faktor för att avskräcka från cyberbrott. Dagens förfaranden måste dock anpassas bättre till internetåldern[65]. Cyberangrepp sker snabbt och kan sätta våra system ur spel, vilket kan skapa särskilda behov av snabbt samarbete över gränserna. Precis som kommissionen informerade om inom ramen för den europeiska säkerhetsagendan kommer den därför tidigt 2018 att lägga ram förslag för att underlätta **gränsöverskridande åtkomst till elektroniska bevis**. Parallellt med detta vidtar kommissionen praktiska åtgärder för att förbättra den gränsöverskridande tillgången till elektroniska bevis för brottsutredningar, bland annat finansiering av utbildning i

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Ett protokoll för sökningar och svar som används allmänt för att söka i databaser som lagrar registrerade användare eller personer som förvärvar internetresurser.

[64] Internet Corporation for Assigned Names and Numbers (ICANN) är en ideell organisation som ansvarar för att samordna underhåll och rutiner för flera databaser som registrerar namnrymder på internet.

[65] För att bara nämna ett exempel bytte den (virtuella) centrala kommando- och kontrollservern i robotnätet Avalanche fysiska servrar och domäner var femte minut.

gränsöverskridande samarbete, utveckling av en elektronisk plattform för informationsutbyte inom EU och standardisering av former av straffrättsligt samarbete mellan medlemsstaterna.

Ett annat hinder för effektiv lagföring är att medlemsstaterna har olika kriminaltekniska förfaranden för insamling av e-bevis i cyberbrottsutredningar. Detta problem kan avhjälpas genom att medlemsstaterna arbetar för att fastställa gemensamma kriminaltekniska standarder. Den kriminaltekniska kapaciteten måste dessutom förstärkas för att stödja spårbarhet och identifiering av skyldiga. En lösning skulle kunna vara att vidareutveckla Europols kriminaltekniska kapacitet och anpassa de befintliga budget- och personalresurserna för Europols europeiska cyberbrottscentrum för att tillgodose det ökande behovet av operativt stöd vid gränsöverskridande cyberbrottsutredningar. En annan lösning skulle vara att tillämpa samma inriktning som ovan för kryptering, eftersom kryptering missbrukas av brottslingar och därmed skapar stora utmaningar i kampen mot grov brottslighet, bland annat terrorism och cyberbrott. Kommissionen kommer att lägga fram resultaten av sina pågående diskussioner om **krypteringens roll i brottsutredningar**[66] i oktober 2017[67].

Med tanke på internets gränslösa natur ger den ram för internationellt samarbete som tillhandahålls genom Europarådets **Budapestkonvention om it-brottslighet**[68] möjligheter för olika länder att använda en optimal rättslig standard för de olika nationella lagstiftningarna mot cyberbrott. Ett eventuellt tilläggsprotokoll till konventionen diskuteras nu[69], som även skulle utgöra en användbar möjlighet att hantera frågan om gränsöverskridande tillgång till elektroniska bevis i ett internationellt sammanhang. I stället för att skapa nya internationella rättsliga instrument för cyberbrott uppmanar EU alla länder att utforma lämplig nationell lagstiftning och samarbeta inom den befintliga internationella ramen.

Den genomgripande tillgången till avidentifieringsverktyg gör det lättare för brottslingarna att gömma sig. ”**Darknet**”[70] har öppnat nya möjligheter för brottslingar att få åtkomst till material med sexuella övergrepp mot barn, narkotika eller skjutvapen, ofta med liten risk för upptäckt[71]. Darknet är nu också en viktig källa till verktyg som används vid cyberbrott, t.ex. sabotageprogramvara och hackningsverktyg. Tillsammans med relevanta intressenter kommer kommissionen att analysera nationella strategier för att hitta nya lösningar. Europol bör underlätta och stödja utredningar på darknet, bedöma hot och bidra till att fastställa behörighet och prioriterade högriskfall, och EU kan spela en ledarroll i samordningen av internationella åtgärder[72].

---

66 Rådets ordförandeskap, resultat av mötet i rådet (rättsliga och inrikes frågor) den 8–9 december 2016, nr 15391/16.

67 *Eighth progress report towards an effective and genuine Security Union* av den 29 juni 2017, COM(2017) 354 final.

68 Konventionen är det första internationella fördraget om brott som begås via internet och andra datanätverk och handlar särskilt om överträdelser av upphovsmannarätten, datorrelaterat bedrägeri, barnpornografi och kränkningar av nätverkssäkerheten. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 År 2017 hade 55 regeringar ratificerat eller anslutit sig till Europarådets konvention om it-brottslighet.

69 *Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, T-CY (2017)3.

70 Darknet består av innehåll i överliggande nätverk som använder internet, men kräver särskild programvara, konfigurationer eller tillstånd för åtkomst. Darknet utgör en liten del av den djupa webben, den del av webben som inte indexeras av sökmotorer.

71 Ett anmärkningsvärt undantag är den senaste tidens stängning av två av de största dark web-marknaderna, AlphaBay och Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Europol spelar redan en viktig roll på detta område. Ett färskt exempel är https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

Ett område som ökar inom cyberbrottsligheten är bedräglig användning av kreditkortsuppgifter eller andra elektroniska betalningsmedel. Identifieringsuppgifter för betalning som har erhållits via cyberangrepp mot näthandlare eller andra lagliga verksamheter handlas på nätet och kan användas av brottslingar för att begå bedrägeri[73]. Kommissionen lägger fram ett förslag för att öka den avskräckande effekten genom ett **direktiv om bekämpande av bedrägeri och förfalskning av andra betalningsmedel än kontanter**[74]. Syftet är att uppdatera de befintliga reglerna på detta område och öka de brottsbekämpande myndigheternas möjligheter att hantera denna form av brott.

Utredningskapaciteten för cyberbrott hos medlemsstaternas brottsbekämpande myndigheter måste också förbättras, och åklagarna och rättsväsendet måste förbättra sin förståelse av cyberbrott och de utredningsalternativ som åklagarna och rättsväsendet har tillgång till. Eurojust och Europol bidrar till detta mål och till förstärkt samordning, i nära samarbete med specialiserade rådgivande grupper inom Europols cyberbrottscentrum och med nätverket för ansvariga för cyberbrottsenheter och åklagare som har specialiserat sig på cyberbrott. Kommissionen kommer att anslå finansiering till ett belopp av 10,5 miljoner euro för bekämpning av cyberbrott, främst inom sitt **polisprogram inom Fonden för inre säkerhet**. Utbildning är en viktig faktor och Ecteg (European Cybercrime Training and Education Group) har tagit fram mycket användbart material. Detta material bör nu spridas allmänt till personal vid brottsbekämpande myndigheter, med stöd från Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol).

3.3 Offentligt-privat samarbete mot cyberbrott

Traditionella brottsbekämpningsmekanismers effektivitet möter problem när det gäller den digitala världens utformning, som främst består av privatägd infrastruktur och omfattar många olika aktörer inom många jurisdiktioner. Därför är samarbete med den privata sektorn, t.ex. näringslivet och det civila samhället, avgörande för att de offentliga myndigheterna effektivt ska kunna bekämpa brott. I detta sammanhang spelar även finanssektorn en avgörande roll och samarbetet bör därför ökas. Finansunderrättelseenheternas[75] roll inom ramen för cyberbrottslighet bör till exempel stärkas.

Vissa medlemsstater har redan vidtagit viktiga åtgärder. I Nederländerna arbetar finansinstitut och brottsbekämpande myndigheter sida vid sida i arbetsgruppen för elektronisk brottslighet för att hantera nätbedrägerier och cyberbrottslighet. Det tyska kompetenscentrumet mot cyberbrott utgör den operativa knutpunkten för dess medlemmar, där de kan utbyta information i nära samarbete med den tyska federala polisen och utforma åtgärder till skydd mot cyberbrott. Sexton medlemsstater[76] har inrättat expertcentrum för cyberbrott för att underlätta samarbetet mellan brottsbekämpande myndigheter, den akademiska världen och privata partner, med målet att utforma och utbyta bästa praxis,

[73] Vinning av bedrägeri är en stor inkomstkälla för organiserad brottslighet och möjliggör därför andra brottsliga verksamheter som terrorism, narkotikahandel och människohandel.

[74] COM(2017) 489.

[75] Finansunderrättelseenheter fungerar som nationella centrum för mottagande och analys av misstänkta transaktionsrapporter och annan information som är relevant för penningtvätt, relaterade förbrott och finansiering av terrorism, och för spridningen av resultaten av sådana analyser.

[76] Belgien, Bulgarien, Cypern, Estland, Frankrike, Förenade kungariket, Grekland, Irland, Litauen, Polen, Rumänien, Slovenien, Spanien, Tjeckien, Tyskland och Österrike.

utbildning och kapacitetsuppbyggnad.
Kommissionen stöder inrättandet av offentlig-privata partnerskap och samarbetsmekanismer via särskilda projekt som Online Fraud Cyber Centre and Experts Network,[77], som genomför en modell och en standard för informationsutbyte för att analysera och begränsa riskerna för e-brott och nätbedrägerier.

När det gäller cyberbrottslighet måste privata företag kunna utbyta information om konkreta incidenter med brottsbekämpande myndigheter – även personuppgifter – med fullständig respekt för uppgiftsskyddsbestämmelserna. Reformen av EU:s uppgiftsskyddslagstiftning, som kommer att börja tillämpas i maj 2018, består av en gemensam uppsättning regler som anger de förhållanden då brottsbekämpande myndigheter och privata enheter kan samarbeta. Kommissionen kommer att arbeta med Europeiska dataskyddsstyrelsen och relevanta intressenter för att fastställa bästa praxis på detta område och vid behov tillhandahålla vägledning.

3.4 Ökade politiska svarsåtgärder

Den nyligen antagna **ramen för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet**[78] (verktygslådan för cyberdiplomati) anger de åtgärder som kommer att vidtas inom den gemensamma utrikes- och säkerhetspolitiken, även restriktiva åtgärder som kan användas för att stärka EU:s svarsåtgärder mot aktiviteter som skadar dess politiska, säkerhetsmässiga och ekonomiska intressen. Ramen utgör ett viktigt steg i utvecklingen av varnings- och handlingskapacitet på EU-nivå och nationell nivå. Den kommer att förbättra vår kapacitet att hitta de skyldiga till skadliga cyberaktiviteter, med målet att påverka eventuella angripares beteende, samtidigt som hänsyn tas till behovet av att säkerställa proportionerliga svarsåtgärder. Att hänföra ett brott till en statlig eller icke-statlig aktör förblir ett suveränt politiskt beslut, baserat på alla underrättelsekällor. Arbetet med att genomföra ramen pågår för närvarande ute i medlemsstaterna och kommer även att tas vidare i nära samordning med den konkreta planen för att hantera storskaliga cyberincidenter[79]. Den situationsmedvetenhet som krävs för att vidta åtgärder inom ramen bör sammanställas, analyseras och delas av Intcen,[80] i nära samarbete med medlemsstaterna och EU-institutionerna.

3.5 Bygga upp avskräckningsåtgärder för cybersäkerhet via medlemsstaternas försvarskapacitet

Medlemsstaterna utvecklar redan cyberförsvarskapacitet. EU är väl lämpat att bidra till att främja synergier mellan militära och civila insatser[81] med tanke på de otydliga gränserna mellan cyberförsvar och cybersäkerhet och det faktum att cyberverktyg och cybertekniker har dubbla användningsområden samt de stora skillnaderna mellan medlemsstaternas strategier.

De medlemsstater som har mer avancerad cybersäkerhetskapacitet och är villiga att slå ihop sådan kapacitet kan, med stöd från utrikesrepresentanten, kommissionen och Europeiska försvarsbyrån, överväga att låta cyberförsvar ingå i ett ”permanent strukturerat samarbete”.

[77] Initiativet EU-OF2CEN syftar till att möjliggöra ett systematiskt utbyte av information om internetbedrägerier mellan banker och brottsbekämpande myndigheter på EU-nivå för att förhindra att betalningar görs till bedragare och penningkurirer och för utredning och lagföring av de berörda förövarna. Det samfinansieras av EU (Fonden för inre säkerhet–Polisprogrammet).

[78] http://www.consilium.europa.eu/sv/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

[80] JOIN(2016) 018 final.

[81] EU tolkar cyberrymden som ett insatsområde precis som mark, luft och hav. Cyberförsvarsinsatser omfattar även skydd för och resiliens hos rymdtillgångar och relaterad markinfrastruktur.

Detta kan underbyggas av de åtgärder som anges ovan för att stimulera EU:s industriella kapacitet och strategiska oberoende. EU kan även främja driftskompatibilitet, bland annat genom att underlätta kapacitetsutveckling, samordning av fortbildning och utbildning samt standardisering av tekniker med dubbla användningsområden.

Den gemensamma ramen för att hantera hybridhot, som ofta involverar cyberangrepp, bör även utnyttjas fullständigt, särskilt genom EU:s gemensamma enhet för hybridhot och det nyligen inrättade europeiska centrumet för motverkande av hybridhot i Helsingfors, vars uppdrag är att uppmuntra strategisk dialog samt genomföra forskning och analyser.

EU kommer att lägga förnyad betoning på ramen för EU:s politik för it-försvar från 2014[82] som ett verktyg för att ytterligare integrera cybersäkerhet och cyberförsvar i den gemensamma säkerhets- och försvarspolitiken (GSFP). Cyberresiliensen hos GSFP:s uppdrag och insatser är viktig i sig: standardiserade förfaranden och teknisk kapacitet kommer att utvecklas, som kan stödja både insatta civila och militära uppdrag och insatser och deras respektive strukturer för planerings- och ledningskapacitet samt utrikestjänstens it-tjänsteleverantörer. För att vidareutveckla medlemsstaternas samarbete och bättre vägleda EU:s insatser på detta område kommer Europeiska försvarsbyrån och utrikestjänsten, i samarbete med kommissionens avdelningar, att underlätta kontakter på strategisk nivå mellan medlemsstaternas beslutsfattare på cyberförsvarsområdet. EU kommer även att stödja utvecklingen av europeiska cybersäkerhetslösningar som ett led i sina insatser för det europeiska försvarets industriella och tekniska bas. Här ingår att främja regionala spetsforskningskluster för cybersäkerhet och försvar.

I nära samarbete med utrikestjänsten, medlemsstaterna och andra relevanta EU-organ kommer kommissionen senast 2018 att inrätta en **utbildningsplattform för cyberförsvar** för att komma till rätta med det rådande kompetensunderskottet inom cyberförsvar. Denna insats kommer att komplettera Europeiska försvarsbyråns arbete på detta område, och bidra till att hantera det rådande kompetensunderskotet inom cybersäkerhet och cyberförsvar.

Viktiga åtgärder

- Ett kommissionsinitiativ för gränsöverskridande åtkomst till elektroniska bevis (tidigt 2018).
- Snabbt antagande av Europaparlamentet och rådet av förslaget till direktiv om bekämpande av bedrägeri och förfalskning av andra betalningsmedel än kontanter**.**
- Införande av krav på IPv6 i EU:s offentliga upphandlingar samt forsknings- och projektfinansiering, frivilliga avtal mellan medlemsstaterna och internetleverantörer för att öka användningen av IPv6.
- Förnyad/breddad inriktning hos Europol på kriminaltekniska frågor i samband med cyberbrott och övervakning av darknet.
- Genomförande av en ram för gemensamma diplomatiska svarsåtgärder på EU-nivå mot skadliga cyberaktiviteter.
- Ökat ekonomiskt stöd till nationella och transnationella projekt som syftar till att förbättra straffrätten i cyberrymden.
- En cybersäkerhetsrelaterad utbildningsplattform 2018 för att komma till rätta med det rådande kompetensunderskottet i fråga om cybersäkerhet och cyberförsvar.

4. STÄRKA DET INTERNATIONELLA SAMARBETET OM CYBERSÄKERHET

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

EU:s internationella cybersäkerhetspolitik vägleds av EU:s kärnvärderingar och grundläggande rättigheter, såsom yttrandefrihet och rätten till integritet och skydd av personuppgifter, samt främjandet av en öppen, fri och säker cyberrymd. Den är utformad för att hantera den ständigt utvecklande utmaningen att främja global cyberstabilitet och bidra till Europas strategiska oberoende i cyberrymden.

4.1 Cybersäkerhet i yttre förbindelser

Belägg visar att människor i hela världen anser att cyberangrepp från andra länder är ett av de största hoten mot nationell säkerhet[83]. Med tanke på hotets globala natur är skapande och upprätthållande av robusta allianser och partnerskap med tredjeländer en grundläggande faktor för förebyggande och avskräckande från cyberangrepp, som blir en alltmer central fråga för internationell stabilitet och säkerhet. EU kommer att prioritera inrättandet av en strategisk ram för konfliktförebyggande och stabilitet i cyberrymden i sina bilaterala, regionala och multilaterala förbindelser och i flerpartsforum.

EU är en stark förespråkare för att internationell rätt, och särskilt FN-stadgan, ska gälla i cyberrymden. Som ett komplement till bindande internationell rätt stöder EU frivilliga icke-bindande normer, regler och principer för ansvarsfullt statligt beteende, som har tagits fram av FN:s grupp av regeringsexperter[84]. EU främjar också utveckling och genomförande av regionala förtroendebyggande åtgärder, både inom Organisationen för säkerhet och samarbete i Europa och i andra regioner.

På bilateral nivå kommer cyberdialoger[85] att vidareutvecklas och kompletteras genom insatser för att underlätta samarbetet med tredjeländer, i syfte att förstärka principerna om tillbörlig aktsamhet och statligt ansvar i cyberrymden. EU kommer att prioritera internationella säkerhetsfrågor i cyberrymden i sina internationella engagemang, samtidigt som det säkerställs att cybersäkerhet inte blir en förvändning för marknadsskydd och begränsningar av grundläggande fri- och rättigheter, bland annat yttrandefriheten och rätten till tillgång till information. En heltäckande strategi för cybersäkerhet kräver respekt för de mänskliga rättigheterna, och EU kommer att fortsätta att upprätthålla sina kärnvärderingar globalt genom att bygga på EU:s riktlinjer för mänskliga rättigheter både online och offline[86]. I detta sammanhang betonar EU betydelsen av att alla intressenter deltar i styrningen av internet.

Kommissionen har också lagt fram ett förslag[87] för att modernisera EU:s exportkontroller, bland annat införande av kontroller av export av kritisk it-övervakningsteknik som kan orsaka kränkningar av de mänskliga rättigheterna eller om den missbrukas utgör en risk för EU:s säkerhet, och kommer att intensifiera dialogerna med tredjeländer för att främja global konvergens och ansvarsfullt agerande på detta område.

4.2 Kapacitetsuppbyggnad på cybersäkerhetsområdet

Den globala cyberstabiliteten är beroende av alla länders lokala och nationella förmåga att förebygga och reagera på cyberincidenter och utreda och lagföra cyberbrott. Stöd till insatser för att bygga upp nationell resiliens i tredjeländer kommer att bidra till att öka cybersäkerheten globalt, med positiva konsekvenser för EU. För att kunna motverka de snabbt utvecklande cyberhoten krävs insatser inom utbildning, politik och utveckling av lagstiftning

[83] *Spring 2017 Global Attitudes Survey*, Pew Research Centre.
[84] A/68/98 och A/70/174.
[85] I september 2017 förde EU cyberdialoger med USA, Kina, Japan, Sydkorea och Indien.
[86] EU Human Rights Guidelines on Freedom of Expression Online and Offline.
[87] COM(2016) 616.

samt effektivt fungerande incidenthanteringsorganisationer och cyberbrottsenheter i världens alla länder.

EU har varit ledande i internationell kapacitetsuppbyggnad på cybersäkerhetsområdet sedan 2013, och kopplar systematiskt dessa insatser till sitt utvecklingssamarbete. EU kommer att fortsätta att främja en rättighetsbaserad kapacitetsuppbyggnadsmodell i linje med strategin Digital4Development[88]. Prioriteringarna för kapacitetsuppbyggnad kommer att vara EU:s grannskap och utvecklingsländer där internetanslutningen ökar i hög takt och hoten utvecklas snabbt. EU:s insatser på detta område kommer att komplettera EU:s utvecklingsagenda mot bakgrund av Agenda 2030 för hållbar utveckling och de övergripande insatserna för institutionell kapacitetsuppbyggnad.

För att förbättra EU:s förmåga att samla all gemensam sakkunskap för att stödja kapacitetsuppbyggnad bör ett särskilt EU-nätverk för kapacitetsuppbyggnad på cyberområdet inrättas, som sammanför utrikestjänsten, medlemsstaternas cybermyndigheter, EU-organ, kommissionens avdelningar, den akademiska världen och det civila samhället. EU-riktlinjer för kapacitetsuppbyggnad på cyberområdet kommer att utformas för att ge bättre politisk vägledning och prioritera EU:s insatser för att hjälpa tredjeländer.

EU kommer även att samarbeta med andra givare på detta område i syfte att undvika dubbelarbete och underlätta mer riktad kapacitetsuppbyggnad i olika regioner.

4.3 Samarbete mellan EU och Nato

Genom att bygga vidare på de viktiga framsteg som redan har gjorts kommer EU att fördjupa sitt samarbete med Nato om cybersäkerhet, hybridhot och försvar enligt den gemensamma förklaringen av den 8 juli 2016[89]. Några av prioriteringarna är att främja interoperabilitet genom enhetliga krav och standarder för cyberförsvar, stärka samarbetet om träning och övningar och att harmonisera utbildningskraven.

EU och Nato kommer även att främja forskning om cyberförsvar och samarbete om innovation, samt bygga vidare på det gällande tekniska arrangemanget för informationsutbyte om cybersäkerhet mellan sina respektive cybersäkerhetsorgan[90]. Den senaste tidens gemensamma insatser för att motverka cyberhot, särskilt samarbetet mellan EU:s gemensamma enhet för hybridhot och Natos Hybrid Analysis Branch, bör utökas ytterligare för att stärka resiliensen och svarsåtgärderna vid cyberkriser. Ytterligare samarbete mellan EU och Nato kommer att främjas genom cyberförsvarsövningar, med deltagande av utrikestjänsten, andra EU-enheter och de relevanta motparterna i Nato, bland annat Natos Cooperative Cyber Defence Centre of Excellence i Tallinn. För första gången kommer Nato och EU att genomföra parallella och samordnade övningar till svar på ett hybridscenario, där Nato tar ledningen 2017 och EU ansvarar på liknande sätt 2018. Nästa rapport om samarbetet mellan EU och Nato, som ska läggas fram för de respektive rådskonstellationerna i december 2017, kommer att vara ett tillfälle att överväga möjligheterna att ytterligare utöka samarbetet, särskilt genom att säkerställa gemensamma, säkra och robusta kommunikationskanaler mellan alla berörda relevanta institutioner och organ, inklusive Enisa.

Viktiga åtgärder

- Göra framsteg med den strategiska ramen för konfliktförebyggande och stabilitet i cyberrymden.

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/sv/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] Cert-EU och Natos Computer Incident Response Capability (NCIRC).

- Utveckla ett nytt nätverk för kapacitetsuppbyggnad för att stödja tredjeländers förmåga att hantera cyberhot samt ta fram EU-riktlinjer för kapacitetsuppbyggnad på cybersäkerhetsområdet för att bättre prioritera EU:s insatser.
- Utöka samarbetet mellan EU och Nato, bland annat genom deltagande i parallella och samordnade övningar och förbättrad interoperabilitet för cybersäkerhetsstandarder.

5. SLUTSATS

EU:s cyberberedskap är central för både den digitala inre marknaden och för vår säkerhets- och försvarsunion. Att förbättra Europas cybersäkerhet och hantera hot mot både civila och militära mål är ett måste.

Det kommande digitala toppmötet, som anordnas av det estländska ordförandeskapet den 29 september 2017, utgör ett tillfälle att visa en gemensam beslutsamhet att sätta cybersäkerhet i centrum för EU som ett digitalt samhälle. Som en del av detta gemensamma åtagande uppmanar kommissionen medlemsstaterna att förklara hur de har för avsikt att agera inom de områden där de har det primära ansvaret. Detta bör omfatta att stärka cybersäkerheten genom att

- säkerställa ett fullständigt och effektivt genomförande av direktivet om nät- och informationssäkerhet senast den 9 maj 2018 och säkerställa nödvändiga resurser för de offentliga myndigheter som ansvarar för cybersäkerhet så att de kan utföra sina uppgifter på ett effektivt sätt,
- tillämpa samma regler för offentliga förvaltningar, med tanke på den roll de spelar i samhället och i ekonomin i stort,
- tillhandahålla cybersäkerhetsrelaterad fortbildning vid offentliga förvaltningar,
- prioritera cybermedvetande i informationskampanjer och integrera cybersäkerhet i akademiska och yrkesinriktade kursplaner,
- använda initiativ inom det permanenta strukturerade samarbetet och Europeiska försvarsfonden för att stödja utvecklingen av cyberförsvarsprojekt.

Detta gemensamma meddelande beskriver utmaningens omfattning och de olika åtgärder som EU kan vidta. Vi behöver ett resilient Europa, som kan skydda sitt folk på ett effektivt sätt genom att föregripa möjliga cybersäkerhetsincidenter, bygga upp ett starkt skydd i sina strukturer och i sitt agerande genom att snabbt återhämta sig från cyberangrepp och avskräcka personer som begår sådana brott. Detta meddelande innehåller riktade åtgärder som ytterligare kommer att stärka EU:s strukturer och kapacitet på cybersäkerhetsområdet på ett samordnat sätt, i fullständigt samarbete med medlemsstaterna och de olika berörda EU-strukturerna, samtidigt som deras befogenheter och ansvarsuppgifter respekteras. Genomförandet av detta meddelande kommer att tydligt visa att EU och dess medlemsstater kommer att arbeta tillsammans för att införa en cybersäkerhetsstandard som motsvarar de växande utmaningar som Europa står inför i dag.