Europeiska unionens råd

Bryssel den 16 december 2020
(OR. en)

14133/20

Interinstitutionellt ärende:
2020/0305 (NLE)

CYBER 280	RECH 529
JAI 1118	COMPET 642
JAIEX 121	IND 273
EJUSTICE 107	COTER 115
COSI 254	ENFOPOL 350
DATAPROTECT 154	COPS 485
COPEN 387	MI 578
TELECOM 269	IXIM 139
PROCIV 99	POLMIL 201
CSC 367	HYBRID 48
CIS 65	CSCI 96
RELEX 1019	POLGEN 234

FÖLJENOT

från:	Europeiska kommissionens generalsekreterare, undertecknat av Martine DEPREZ, direktör
inkom den:	16 december 2020
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	JOIN(2020) 18 final
Ärende:	GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET EU:s strategi för cybersäkerhet för ett digitalt decennium

För delegationerna bifogas dokument – JOIN(2020) 18 final.

Bilaga: JOIN(2020) 18 final

EUROPEISKA KOMMISSIONEN

UNIONENS HÖGA REPRESENTANT FÖR UTRIKES FRÅGOR OCH SÄKERHETSPOLITIK

Bryssel den 16.12.2020
JOIN(2020) 18 final

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET

EU:s strategi för cybersäkerhet för ett digitalt decennium

GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET

EU:s strategi för cybersäkerhet för ett digitalt decennium

I. INLEDNING EN CYBERSÄKER DIGITAL OMSTÄLLNING I EN KOMPLEX HOTMILJÖ

Cybersäkerheten är en integrerad del av EU-medborgarnas säkerhet. Oavsett om det handlar om enheter eller elnät som de använder, eller banker, flyg, offentliga förvaltningar eller sjukhus som de besöker, ska de kunna göra detta i förvissning om att de är skyddade från cyberhot. EU:s ekonomi, demokrati och samhälle är mer beroende än någonsin av säkra och tillförlitliga digitala verktyg och uppkopplingar. Därför är cybersäkerheten avgörande för att bygga ett motståndskraftigt, grönt och digitalt Europa.

Transport, energi, hälso- och sjukvård, telekommunikationer, finans och säkerhet, de demokratiska processerna, rymden och försvaret är kraftigt beroende av nätverks- och informationssystem som blir allt mer sammankopplade. Det råder mycket starka sektorsövergripande ömsesidiga beroenden, eftersom nät- och informationssystemen i sin tur är beroende av en stabil elförsörjning för att fungera. Antalet uppkopplade enheter är redan större än antalet människor på jorden, och förväntas öka till 25 miljarder fram till 2025[1]: en fjärdedel av dessa kommer att finnas i Europa. Digitaliseringen av arbetsmönstren har påskyndats av covid-19-pandemin, då 40 % av EU:s arbetstagare övergick till distansarbete, vilket sannolikt kommer att ha bestående effekter på vardagslivet[2]. Detta ökar sårbarheten för cyberattacker[3]. Uppkopplade föremål levereras ofta till konsumenten med kända sårbarheter, vilket ytterligare ökar attackytan för skadlig cyberverksamhet[4]. Industrilandskapet i EU blir alltmer digitaliserat och uppkopplat. Detta innebär också att cyberattacker kan få större inverkan på branscher och ekosystem än någonsin tidigare.

Hotbilden förvärras av de geopolitiska spänningarna kring ett globalt och öppet internet och kring kontrollen över tekniken i hela leveranskedjan[5]. Dessa spänningar återspeglas i det ökande antalet nationalstater som upprättar digitala gränser. Restriktionerna av och på internet hotar den globala och öppna cyberrymden och rättsstatsprincipen, de

---

[1] Uppskattning gjord av branschorganisationen GSMA för telekommunikationer, https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). International Data Corporation förutser 42,6 miljarder uppkopplade maskiner, sensorer och kameror, https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Enligt en enkät från juni 2020 uppgav 47 % av företagsledarna att de har för avsikt att låta de anställda arbeta på distans på heltid även när det blir möjligt att återvända till arbetsplatsen: 82 % hade för avsikt att tillåta distansarbete åtminstone en del av tiden. https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Ett av de skadligaste sabotageprogrammen hittills, känt som Mirai, skapade botnät bestående av över 600 000 enheter som störde flera stora webbplatser i Europa och USA.

[5] Till exempel elektroniska komponenter, dataanalys, moln, snabbare och smartare nätverk med 5G och senare teknik, kryptering, artificiell intelligens (AI) och nya dataparadigm och betrodda paradigm för databehandling såsom blockkedjeteknik, cloud-to-edge och kvantdatorteknik.

grundläggande rättigheterna, friheten och demokratin – EU:s grundläggande värden. Cyberrymden utnyttjas alltmer för politiska och ideologiska ändamål, och ökad polarisering på internationell nivå hindrar effektiv multilateralism. Hybridhot kombinerar desinformationskampanjer med cyberattacker på infrastruktur, ekonomiska processer och demokratiska institutioner, som kan förorsaka fysisk skada, olaglig tillgång till personuppgifter, stöld av industri- eller statshemligheter, misstro och försvagning av den sociala sammanhållningen. Denna verksamhet undergräver den internationella säkerheten och stabiliteten och de fördelar som cyberrymden för med sig för den ekonomiska, sociala och politiska utvecklingen.

De skadliga angreppen på kritisk infrastruktur är en stor global risk[6]. Internet har en decentraliserad struktur utan central struktur och med flerpartsstyre. Det har lyckats med att registrera kontinuerliga exponentiella ökningar av trafikvolymen samtidigt som det varit ett konstant mål för skadliga störningsförsök[7]. Samtidigt ökar beroendet av de centrala funktionerna hos ett globalt och öppet internet, såsom domännamnssystemet (DNS) och samhällsviktiga internettjänster för kommunikation och värdtjänster, tillämpningar och data. Dessa tjänster koncentreras alltmer till ett fåtal privata företag[8]. Det gör den europeiska ekonomin och det europeiska samhället sårbara för störande geopolitiska eller tekniska händelser som påverkar kärnan av Internet eller ett eller flera av dessa företag. Den ökade internetanvändningen och de förändrade mönstren till följd av pandemin har ytterligare blottlagt sårbarheten i de leveranskedjor som är beroende av denna digitala infrastruktur.

Farhågor rörande säkerheten är ett negativt incitament för att använda onlinetjänster[9]**.** Omkring två femtedelar av användarna i EU har upplevt säkerhetsrelaterade problem och tre femtedelar känner sig oförmögna att skydda sig mot cyberbrottslighet[10]. En tredjedel har fått bedrägliga e-postmeddelanden eller telefonsamtal med begäran om personuppgifter under de senaste tre åren, men 83 % har aldrig rapporterat något cyberbrott. Vart åttonde företag har drabbats av cyberattacker[11]. Över hälften av de persondatorer tillhörande företag och konsumenter som har smittats med sabotageprogram infekteras på nytt samma år[12]. Hundratals miljoner uppgifter går förlorade varje år till följd av dataintrång, och den genomsnittliga kostnaden för en överträdelse för ett enskilt företag steg till över 3,5 miljoner

---

[6] World Economic Forum, Global Risks Report 2020.

[7] Pandemin ledde till en ökning av internettrafiken med 60 % enligt Organisationen för ekonomiskt samarbete och utveckling (OECD); https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/ Byrån för Organet för europeiska regleringsmyndigheter för elektronisk kommunikation och kommissionen offentliggör regelbundet rapporter om internetkapaciteten under isoleringsåtgärderna till följd av covid-19-pandemin. Enligt en rapport från Enisa ökade det totala antalet samordnade överbelastningsattacker (DDoS) med 241 % under tredje kvartalet 2019 jämfört med tredje kvartalet 2018. DDoS ökar i intensitet, och den största attacken någonsin ägde rum i februari 2020 och nådde en trafiktäthet på 2,3 terabits per sekund. Vid ”CenturyLink-avbrottet” i augusti 2020 ledde ett dirigeringsproblem hos den amerikanska internetleverantören CenturyLink till en minskning av den globala webbtrafiken med 3,5 %. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8] Internet Society, The Global Internet Report: Consolidation in the Internet Economy, https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[10] 2020 Digital Economy and Society Index, https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Eurostats pressmeddelande ”ICT security measures taken by vast majority of enterprises in the EU”, 6/2020 – 13 januari 2020. ”Cyberattacker mot kritisk infrastruktur har blivit den nya normala inom sektorer som energi, hälso- och sjukvård och transport”, WEF, The Global Risks Report 2020.

[12] Källa: Comparitech.

euro 2018[13]. Inverkan av en cyberattack kan ofta inte isoleras och kan utlösa kedjereaktioner i hela ekonomin och samhället, vilket påverkar miljontals människor[14].

Utredningar av nästan alla typer av brott har en digital komponent. Under 2019 rapporterades antalet incidenter från ett år till ett annat ha tredubblats. Det finns uppskattningsvis 700 miljoner nya prover på sabotageprogram – det vanligaste sättet att genomföra en cyberattack[15]. Den globala ekonomins årliga kostnad för cyberbrottslighet 2020 uppskattas till 5,5 biljoner euro, vilket är dubbelt så mycket som 2015[16]. Detta är den största överföringen av ekonomiskt välstånd i historien, större än den globala narkotikahandeln. För en omfattande incident, attacken med utpressningsprogrammet WannaCry 2017, uppskattades kostnaden för den globala ekonomin till över 6,5 miljarder euro[17].

Digitala tjänster och finanssektorn är de som oftast utsätts för cyberattacker, liksom den offentliga sektorn och tillverkningsindustrin, och ändå är beredskapen och medvetenheten bland företagen och enskilda fortfarande låg[18], och det råder en betydande kompetensbrist när det gäller cybersäkerhet bland arbetskraften[19]. Under 2019 inträffade nästan 450 cybersäkerhetsincidenter som rörde europeisk kritisk infrastruktur såsom finans och energi[20]. Hälso- och sjukvårdsorganisationerna och vårdpersonalen har drabbats särskilt hårt under pandemin. I takt med att tekniken och den fysiska världen blir oupplösligt sammankopplade äventyrar cyberattackerna de mest utsattas liv och välbefinnande[21]. Mer än två tredjedelar av företagen, särskilt de små och medelstora företagen, anses vara ”amatörer” inom cybersäkerhet, och de europeiska företagen anses mindre väl förberedda än företagen i Asien och Amerika[22]. Uppskattningsvis 291 000 tjänster för cybersäkerhetspersonal i Europa är fortfarande otillsatta. Att anställa och utbilda experter på cybersäkerhet är en långsam process som leder till större cybersäkerhetsrisker för organisationerna[23].

EU saknar en kollektiv situationsmedvetenhet om cyberhot. Detta beror på att de nationella myndigheterna inte systematiskt samlar in och utbyter information – till exempel information från den privata sektorn – som skulle kunna bidra till att bedöma

---

[13] Rapporten *Annual Cost of a Data Breach Report*, 2020 Ponemon Institute, och baserat på en kvantitativ analys av 524 nyligen inträffade intrång inom 17 geografiska områden och 17 branscher. https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Rapport från gemensamma forskningscentrumet (JRC), *Cybersecurity, our digital anchor*. https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Källa: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] JRC, Cybersecurity – Our Digital Anchor.

[17] Källa: Cyence.

[18] Företagens medvetenhet är även låg när det gäller cyberstölder av företagshemligheter, särskilt bland de små och medelstora företagen. PwC, *Study on the scale and impact of industrial espionage and theft of trade secrets through cyber: Dissemination report on measures to tackle and prevent cyber-theft of trade secrets*, 2018.

[19] Se Enisa *Threat Landscape 2020*. Även Verizon *Data Breach Investigations Report 2020*, https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Utpressningsprogram har använts för att angripa sjukhus och patientjournaler, t.ex. i Rumänien (juni 2020), Düsseldorf (september 2020) och Vastaamo (oktober 2020).

[22] PwC, The Global State of Information Security 2018; ESI Thoughtlab, The Cybersecurity Imperative, 2019.

[23] EU:s cybersäkerhetsbyrå, *Cybersecurity Skills Development in the EU*: *The certification of cybersecurity degrees and ENISA's Higher Education Database*, dcember 2019.

cybersäkerhetssituationen i EU. Endast en bråkdel av incidenterna rapporteras av medlemsstaterna, och informationsutbytet är varken systematiskt eller heltäckande[24]. Det kan hända att cyberattackerna endast utgör en aspekt av samordnade skadliga angrepp mot europeiska samhällen. Det förekommer för närvarande endast begränsat ömsesidigt operativt bistånd mellan medlemsstaterna, och det finns ingen operativ mekanism mellan medlemsstaterna och EU:s institutioner, byråer och organ i händelse av storskaliga, gränsöverskridande cyberincidenter eller cyberkriser[25].

Att förbättra cybersäkerheten är därför avgörande för att människor ska kunna lita på, använda och dra nytta av innovation, konnektivitet och automatisering, och för att skydda de grundläggande fri- och rättigheterna, inbegripet rätten till integritet och skydd av personuppgifter och yttrande- och informationsfriheten. Cybersäkerheten är oumbärlig för den nätkonnektivitet och det globala och öppna internet som måste ligga till grund för omvandlingen av ekonomin och samhället under 2020-talet. Den bidrar till fler och bättre arbetstillfällen, flexiblare arbetsplatser, effektivare och hållbarare transporter och jordbruk samt enklare och rättvisare tillgång till hälso- och sjukvårdstjänster. Den är också viktig för omställningen till renare energi inom ramen för den europeiska gröna given[26], genom gränsöverskridande nät och smarta mätare och för att undvika onödig dubblering av datalagring. Slutligen är den viktig för den internationella säkerheten och stabiliteten och för utvecklingen av ekonomier, demokratier och samhällen i hela världen. Regeringarna, företagen och de enskilda måste därför använda de digitala verktygen på ett ansvarsfullt och säkerhetsmedvetet sätt. Medvetenhet och cybersäkerhet och cybersäkerhetshygien måste ligga till grund för den digitala omställningen av de vardagliga aktiviteterna.

EU:s nya cybersäkerhetsstrategi för det digitala decenniet är en central del av utformningen av EU:s digitala framtid[27], kommissionens återhämtningsplan för EU[28], EU:s strategi för säkerhetsunionen 2020–2025[29], den globala strategin för Europeiska unionens utrikes- och säkerhetspolitik[30], och Europeiska rådets strategiska agenda för 2019–2024[31]. Den anger hur EU kommer att skydda sina medborgare, företag och institutioner från cyberhot och hur EU kommer att främja internationellt samarbete och leda arbetet med att säkra ett globalt och öppet internet.

II. ATT TÄNKA GLOBALT OCH AGERA EUROPEISKT

Den här strategin syftar till att säkerställa ett globalt och öppet internet försett med kraftiga skyddsräcken för att hantera riskerna för EU-invånarnas säkerhet och grundläggande fri- och rättigheter. Efter framstegen med de tidigare strategierna innehåller den här strategin konkreta förslag på tre huvudinstrument – ett lagstiftningsinstrument, ett investeringsinstrument och ett politiskt instrument — som ska sättas in på tre områden för EU-insatser – 1) resiliens, teknisk suveränitet och ledarskap, 2) operativ kapacitet för att förebygga, motverka och bemöta, och (3) främjande av en global och öppen cyberrymd. EU är fast beslutet att stödja denna strategi

[24] I enlighet med artikel 10.3 i direktivet om säkerhet i nätverks- och informationssystem (direktiv (EU) 2016/1148) ska medlemsstaterna lämna en årlig sammanfattande rapport till samarbetsgruppen om de rapporter som mottagits.
[25] Standardrutiner finns för ömsesidigt bistånd mellan medlemmarna i CSIRT-nätverket.
[26] Den europeiska gröna given (COM(2019) 640 final).
[27] Att forma Europas digitala framtid, COM (2020) 67 final.
[28] EU vid ett vägskäl - bygga upp och bygga nytt för nästa generation (COM(2020) 98 final).
[29] EU:s strategi för säkerhetsunionen 2020–2025, COM (2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/#

genom en **aldrig tidigare skådad investeringsnivå i EU:s digitala omställning under de kommande sju åren** - potentiellt en fyrdubbling av tidigare nivåer - som en del av ny teknik- och industripolitik och återhämtningsagendan[32].

Cybersäkerhet måste integreras i alla dessa digitala investeringar, särskilt viktig teknik som artificiell intelligens (AI), kryptering och kvantdatorteknik, med hjälp av incitament, skyldigheter och riktmärken. Detta kan stimulera tillväxten i den europeiska cybersäkerhetssektorn och skapa den säkerhet som behövs för att underlätta utfasningen av äldre system. Europeiska försvarsfonden kommer att stödja europeiska cyberförsvarslösningar, som en del av den europeiska försvarstekniska och försvarsindustriella basen. Cybersäkerhet inkluderas i de externa finansieringsinstrumenten för att stödja våra partner, särskilt instrumentet för grannskapspolitik, utvecklingssamarbete och internationellt samarbete. Förebyggande av teknikmissbruk, skydd av kritisk infrastruktur och säkerställande av leveranskedjornas integritet gör det också möjligt för EU att ansluta sig till FN:s normer, regler och principer för ansvarsfullt statligt agerande[33].

1. Resiliens, teknisk suveränitet och ledarskap

EU:s kritiska infrastruktur och samhällsviktiga tjänster blir allt mer beroende av varandra och digitaliserade. Alla internetanslutna saker i EU, oavsett av om det rör sig om automatiserade bilar, industriella kontrollsystem eller hushållsapparater, och alla leveranskedjor som gör dem tillgängliga, måste ha inbyggd säkerhet (*secure-by-design*), motståndskraftiga mot cyberincidenter och snabbt kunna förses med programfixar när sårbarheter upptäcks. Detta är avgörande för att ge EU:s privata och offentliga sektor möjlighet att välja bland de säkraste infrastrukturerna och tjänsterna. Det kommande decenniet är EU:s möjlighet att bli ledande i utveckling av säker teknik i hela leveranskedjan. För att säkerställa resiliens och starkare industriell och teknisk kapacitet i fråga om cybersäkerhet bör alla nödvändiga reglerings-, investerings- och policyinstrument mobiliseras. Att ta hänsyn till cybersäkerhet vid produktens utformning, *cybersecurity by design*, för industriella processer, operationer och anordningar kan minska riskerna och potentiellt minska kostnaderna för såväl företag som samhället i stort, och därmed öka resiliensen.

1.1. Resiliens hos infrastruktur och kritiska tjänster

EU:s **regler om säkerhet i nätverks- och informationssystem** ingår i kärnan av den inre marknaden för cybersäkerhet. Kommissionen föreslår att dessa regler ses över inom ramen för ett reviderat cybersäkerhetsdirektiv för att öka **cyberresiliensen hos alla relevanta sektorer, både offentliga och privata, som fyller en viktig funktion för ekonomin och samhället[34].** Översynen är nödvändig för att minska den bristande enhetligheten på den inre marknaden genom att anpassa tillämpningsområdet, säkerhets- och incidentrapporteringsskyldigheterna, den nationella tillsynen och tillämpningen samt de behöriga myndigheternas kapacitet.

---

[32] Investeringarna i hela försörjningskedjan för digital teknik bör uppgå till minst 20 % - motsvarande 134,5 miljarder euro - av faciliteten för återhämtning och resiliens som uppgår till 672,5 miljarder euro i lån och bidrag. I den fleråriga budgetramen 2021–2027 planeras EU-finansiering för cybersäkerhet inom programmet för ett digitalt Europa, och för cybersäkerhetsforskning inom ramen för Horisont Europa, med särskilt fokus på stöd till små och medelstora företag, kan den uppgå till totalt 2 miljarder euro plus medlemsstaternas och industrins investeringar.

[33] https://undocs.org/A/70/174

[34] [*infoga hänvisning till NIS-förslag*]

Ett reviderat NIS-direktiv kommer att utgöra en grund för mer specifika regler som också behövs för strategiskt viktiga sektorer, bland annat energi, transport och hälsa. För att säkerställa en enhetlig strategi i enlighet med strategin för EU:s säkerhetsunion 2020–2025 föreslås det reformerade direktivet tillsammans med en översyn av lagstiftningen om resiliensen hos kritisk infrastruktur[35]. Energiteknik som innehåller digitala komponenter och säkerheten i de därmed sammanhängande leveranskedjorna är viktiga för kontinuiteten i samhällsviktiga tjänster och för den strategiska kontrollen av kritisk energiinfrastruktur. Kommissionen kommer därför att föreslå åtgärder, inklusive ”nätföreskrifter” med regler för cybersäkerhet i gränsöverskridande elflöden, som ska antas senast i slutet av 2022. Finanssektorn måste också stärka den digitala operativa resiliensen och säkerställa förmågan att stå emot alla typer av IKT-relaterade störningar och hot, såsom kommissionen har föreslagit[36]. På transportområdet har kommissionen lagt till bestämmelser om cybersäkerhet[37] i EU:s lagstiftning om luftfartsskydd och kommer att fortsätta sina insatser för att öka cyberresiliensen inom alla transportsätt. Att stärka cyberresiliensen hos de **demokratiska processerna och institutionerna** är en central del av EU:s handlingsplan för demokrati för att skydda och främja fria val, samt den demokratiska debatten och mediemångfalden[38]. När det gäller säkerheten för infrastruktur och tjänster inom ramen för det framtida rymdprogrammet kommer kommissionen att fortsätta att fördjupa Galileos strategi för cybersäkerhet för nästa generation av globala satellitnavigeringssystem och andra nya komponenter i rymdprogrammet[39].

1.2. Att bygga upp en europeisk cybersköld

Mot bakgrund av den utbredda konnektiviteten och de allt mer sofistikerade cyberattackerna fyller informations- och analyscentralerna en värdefull funktion, även på sektorsnivå, när det gäller att möjliggöra informationsutbyte mellan flera berörda parter om cyberhot[40]. Dessutom krävs det ständig övervakning och analys för att nätverken och datorsystemen ska kunna upptäcka intrång och anomalier i realtid. Många privata företag, offentliga organisationer och nationella myndigheter har därför inrättat cyberincidentcentrum (CSIRT) och säkerhetscentrum.

Säkerhetscentrumen är avgörande för att samla in loggar[41] och isolera misstänkta händelser som inträffar i de kommunikationsnät som de övervakar. De gör detta genom signal- och mönsterigenkänning och kunskapsextraktion rörande brottet från de stora mängder data som behöver bedömas. De har bidragit till att upptäcka skadliga körbara filer och har i sin tur bidragit till att hålla cyberattackerna under kontroll. Det arbete som måste uträttas i dessa centraler är mycket krävande och sker i högt tempo, vilket är anledningen till att AI och i

[35] [infoga hänvisning till *förslaget* till direktiv om kritiska enheters motståndskraft]
[36] Förslag till förordning om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014 och (EU) nr 909/2014, COM (2020) 595 final.
[37] Kommissionens genomförandeförordning 2019/1583.
[38] Meddelande om den europeiska handlingsplanen för demokrati, COM (2020) 790. I enlighet med planen, det europeiska nätverket för valsamarbete, kommer medlemsstaternas valnätverk att stödja utsändandet av gemensamma expertgrupper för att motverka hot mot valprocesser, inbegripet cyberhot. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en
[39] Detta inbegriper ett nytt statligt initiativ om statlig satellitkommunikation (Govsatcom) och rymdskrot (SST).
[40] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[41] På ett sådant sätt att de brottsbekämpande myndigheterna och rättsväsendet kan använda dem som bevis.

synnerhet maskininlärningstekniker kan ge ovärderligt stöd till de som verkar inom detta område[42].

Kommissionen föreslår att det ska byggas upp ett **nätverk av säkerhetscentrum i hela EU[43]**, och kommer att främja en förbättring av befintliga centrum och inrättande av nya. Den kommer också att ge stöd till utbildning och kompetensutveckling för personalen som driver centrumen. På grundval av en behovsanalys som genomförs med relevanta berörda parter och stöds av EU:s cybersäkerhetsbyrå (Enisa) skulle den kunna anslå över 300 miljoner euro för att stödja offentlig-privat och gränsöverskridande samarbete för att skapa nationella och sektoriella nätverk, även med deltagande av små och medelstora företag, på grundval av lämplig styrning, datadelning och säkerhetsbestämmelser.

Medlemsstaterna uppmuntras att saminvestera i detta projekt. Centrumen skulle då på ett effektivare sätt kunna dela och korrelera de upptäckta signalerna och skapa högkvalitativ hotinformation som skulle delas med informations- och analyscentralerna och de nationella myndigheterna, vilket skulle möjliggöra en bättre situationsmedvetenhet. Målet skulle vara att i etapper sammankoppla så många centrum som möjligt i hela EU för att skapa samlad kunskap och utbyta bästa praxis. Stöd kommer att ställas till förfogande för dessa centrum för att förbättra incidentdetektion, analys och reaktionshastighet genom toppmodern AI- och maskininlärningskapacitet och kompletterat med superdatorinfrastruktur som utvecklats i EU av det gemensamma företaget för ett europeiskt högpresterande datorsystem[44].

Genom kontinuerligt samarbete kommer detta nätverk att i god tid utfärda varningar om cybersäkerhetsincidenter till myndigheter och alla berörda parter, inklusive den gemensamma cyberenheten (se avsnitt 2.1.). **Den kommer att fungera som en riktig cybersäkerhetsköld för EU** och tillhandahålla ett nätverk av övervakningstorn som kan upptäcka möjliga hot innan de kan orsaka storskaliga skador.

1.3. En ultrasäker kommunikationsinfrastruktur

Europeiska unionens statliga satellitkommunikation[45], som är en del av rymdprogrammet, kommer att tillhandahålla säker och kostnadseffektiv rymdbaserad kommunikationskapacitet för att säkerställa säkerhetskritiska uppdrag och insatser som förvaltas av EU och dess medlemsstater, inbegripet nationella säkerhetsaktörer och EU:s institutioner och byråer.

Medlemsstaterna har åtagit sig att samarbeta med kommissionen för att bygga ut en säker kvantkommunikationsinfrastruktur för Europa[46]. Kvantkommunikationsinfrastrukturen kommer att erbjuda offentliga myndigheter ett helt nytt sätt att överföra konfidentiell information med hjälp av en ultrasäker krypteringsform för att skydda mot cyberattacker, konstruerat med europeisk teknik. Den kommer att bestå av två huvuddelar: befintliga

[42]Källa: undersökning av Ponemon Institute Research, *Improving the Effectiveness of the SOC*, 2019. För studier om användningen av AI i säkerhetscentrumen, se till exempel: Khraisat, A., Gondal, I., Vamplew, P. *et al. Survey of intrusion detection systems: techniques, datasets and challenges*, *Cybersecur* 2**,** 20 (2019).
[43]Mer detaljerade arrangemang för styrning, driftsprinciper och finansiering av dessa centrum, och hur de ska komplettera befintliga strukturer såsom de digitala innovationsknutpunkterna, kommer att utvecklas.
[44]https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking
[45]Govsatcom är en del av unionens rymdprogram.
[46]EuroQCI-deklarationen har undertecknats av de flesta medlemsstater, och utveckling och utbyggnad av infrastruktur kommer att äga rum 2021–2027 med finansiering från Horisont Europa och Ett digitalt Europa, och Europeiska rymdorganisationen, med förbehåll för lämpliga styrningsarrangemang, https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

markbundna fiberkommunikationsnät som kopplar samman strategiska platser på nationell och gränsöverskridande nivå, och sammankopplade rymdsatelliter som täcker hela EU, inklusive dess utomeuropeiska territorier[47]. Detta initiativ för att utveckla och införa nya och säkrare krypteringsformer och utforma nya sätt att skydda kritiska kommunikations- och datatillgångar kan bidra till att skydda känslig information och i sin tur kritisk infrastruktur.

I detta perspektiv och i ett mer långtgående perspektiv kommer kommissionen att undersöka möjligheten att införa ett säkert multiorbitalsystem för konnektivitet. Det skulle bygga vidare på Govsatcom och kvantkommunikationsinfrastrukturen och integrera spetsteknik (Quantum, 5G, AI och edge computing) och följa den mest restriktiva ramen för cybersäkerhet i syfte att stödja secure-by-design-tjänster, såsom tillförlitlig, säker och kostnadseffektiv konnektivitet och krypterad kommunikation för kritisk statlig verksamhet.

1.4. Säkra nästa generations mobila bredbandsnät

De EU-medborgare och företag i EU som använder avancerade och innovativa tillämpningar som möjliggörs av **5G och framtida generationer av nätverk** bör åtnjuta högsta säkerhetsnivå. Tillsammans med kommissionen och med stöd av Enisa har medlemsstaterna med EU:s 5G-verktygslåda [48]från januari 2020 inrättat en övergripande och objektiv riskbaserad strategi för 5G-cybersäkerhet som bygger på en bedömning av möjliga begränsningsplaner och identifiering av de effektivaste åtgärderna. Dessutom håller EU på att konsolidera sin kapacitet inom 5G och över 5G för att undvika beroende och främja en hållbar och diversifierad leveranskedja.

I december 2020 offentliggjorde kommissionen en rapport om konsekvenserna av rekommendationen av den 26 mars 2019 om it-säkerhet i 5G-nät[49]. Den visade att avsevärda framsteg har gjorts sedan man enades om verktygslådan och att de flesta medlemsstater är på väg att slutföra en betydande del av genomförandet av verktygslådan inom en snar framtid, om än med vissa variationer och återstående luckor, vilket redan konstaterats i den lägesrapport som offentliggjordes i juli 2020[50].

I oktober 2020 uppmanade Europeiska rådet EU och medlemsstaterna att ”fullt ut utnyttja 5G-verktygslådan för cybersäkerhet” och ”tillämpa relevanta begränsningar för högriskleverantörer när det gäller nyckeltillgångar som definieras som kritiska och känsliga i EU:s samordnade riskbedömningar”[51].

---

[47]Utvecklingen av en rymddel är nödvändig för att uppnå långdistans-punkt-till-punkt-förbindelse (> 1 000 km) som markbaserad infrastruktur inte kan stödja. Genom att utnyttja kvantmekanikens egenskaper kommer kvantkommunikationsinfrastrukturen inledningsvis att göra det möjligt för parterna att säkert dela slumpmässiga hemliga nycklar för kryptering och dekryptering av meddelanden. Den kommer också att omfatta en test- och efterlevnadsinfrastruktur som kommer att införas för att bedöma om europeiska kvantkommunikationsanordningar och kvantkommunikationssystem överensstämmer med kvantkommunikationsinfrastrukturen och deras certifiering och validering innan de integreras i kvalitetsindexet. Den kommer att utformas för att stödja ytterligare tillämpningar när de når den tekniska mognadsnivå som krävs. Den nuvarande piloten OpenQKD (https://openqkd.eu/) är en föregångare till denna test- och efterlevnadsinfrastruktur.

[48]meddelandet Säker 5G-utbyggnad i EU – Genomförande av EU:s verktygslåda, COM(2020) 50.

[49]Kommissionens rapport om konsekvenserna av kommissionens rekommendation av den 26 mars 2019 om it-säkerhet i 5G-nät, 15 december 2020.

[50]Rapport från samarbetsgruppen för nät- och informationssäkerhet om tillämpningen av verktygslådan, 24 juli 2020.

[51]EUCO 13/20, Slutsatser från det extra mötet i Europeiska rådet (den 1–2 oktober 2020).

Om man ser till framtiden bör EU och dess medlemsstater se till att de identifierade riskerna har begränsats på ett lämpligt och samordnat sätt, särskilt när det gäller målet att minimera exponeringen för högriskleverantörer och undvika beroende av dessa leverantörer på nationell nivå och unionsnivå, och att varje ny betydande utveckling eller risk beaktas. Medlemsstaterna uppmanas att fullt ut utnyttja verktygslådan i sina investeringar i digital kapacitet och konnektivitet.

På grundval av rapporten om konsekvenserna av rekommendationen från 2019 uppmanar kommissionen medlemsstaterna att påskynda arbetet med att slutföra genomförandet av de viktigaste åtgärderna i verktygslådan senast under andra kvartalet 2021. Den uppmanar också medlemsstaterna att tillsammans fortsätta att övervaka de framsteg som görs och säkerställa ytterligare anpassning av metoderna. På EU-nivå kommer tre huvudmål att eftersträvas för att stödja denna process: säkerställa ytterligare konvergens av riskreduceringsstrategierna i hela EU, stödja fortgående kunskapsutbyte och kapacitetsuppbyggnad, och främja en motståndskraftig leveranskedja och andra strategiska EU-säkerhetsmål. Konkreta åtgärder med anknytning till dessa centrala mål anges i det särskilda tillägget till detta meddelande.

Kommissionen kommer att fortsätta sitt nära samarbete med medlemsstaterna för att uppnå dessa mål och åtgärder med stöd av Enisa (se bilagan).

EU:s verktygslåda för 5G har dessutom väckt intresse bland länder utanför EU som för närvarande utvecklar sina strategier för att säkra sina kommunikationsnät. Kommissionen är beredd att, tillsammans med Europeiska utrikestjänsten och nätverket av EU-delegationer, på begäran lämna ytterligare information om sin övergripande, objektiva och riskbaserade strategi till myndigheter runt om i världen.

1.5. Ett säkert sakernas internet

Allt som är uppkopplat innehåller sårbarheter som kan utnyttjas med risk för omfattande konsekvenser. Reglerna för den inre marknaden omfattar skyddsåtgärder mot osäkra produkter och tjänster. Kommissionen arbetar redan för att säkerställa **transparenta säkerhetslösningar och certifiering enligt cybersäkerhetsakten** och för att skapa incitament för framställa säkra produkter och tjänster utan att äventyra prestandan[52]. Den kommer att anta sitt första unionens löpande arbetsprogram under första kvartalet 2021 (vilket ska uppdateras minst vart tredje år) så att industrin, de nationella myndigheterna och standardiseringsorganen kan förbereda sig i förväg inför framtida europeiska ordningar för cybersäkerhetscertifiering[53]. Allteftersom sakernas internet sprider sig måste de verkställbara reglerna stärkas, både för att säkerställa övergripande motståndskraft och för att stärka cybersäkerheten.

Kommissionen kommer att överväga en övergripande strategi, inklusive eventuella **nya horisontella regler för att förbättra cybersäkerheten för alla uppkopplade produkter**

[52] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). Cybersäkerhetsakten främjar IKT-certifiering på EU-nivå genom ett europeiskt ramverk för cybersäkerhetscertifiering för inrättandet av frivilliga europeiska ordningar för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för IKT-produkter, IKT-tjänster och IKT-processer i unionen samt i syfte att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Samtidigt har företag som ”värderar” cybersäkerhet företrädesvis etablerat sig utanför EU med begränsad transparens och tillsyn. https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53] Krävs enligt artikel 47.5 i cybersäkerhetsakten.

och tillhörande tjänster som släpps ut på den inre marknaden[54]. Sådana regler skulle kunna omfatta en **ny aktsamhetsplikt för tillverkare av uppkopplad utrustning för** att ta itu med sårbarheter i programvaran, inbegripet fortsatt uppdatering av programvaran och säkerhetsuppdateringar, samt säkerställa att personuppgifter och andra känsliga uppgifter raderas i slutet av livscykeln. Dessa regler skulle främja ”rätten att få en föråldrad programvara reparerad”, ett initiativ som lades fram i EU:s handlingsplan för den cirkulära ekonomin och kompletterar pågående åtgärder som avser särskilda produkttyper, såsom tvingande krav som ska fastställas för införande på marknaden av vissa trådlösa produkter **(**genom antagande av en delegerad akt inom ramen för direktivet om radioutrustning[55]), och målet att införa cybersäkerhetsregler för motorfordon för alla typer av nya fordon från och med juli 2022[56]. De skulle dessutom bygga vidare på den föreslagna översynen av de allmänna produktsäkerhetsreglerna, som inte direkt berör cybersäkerhetsaspekter[57].

1.6. Stärkt global internetsäkerhet

En uppsättning kärnprotokoll och stödinfrastruktur säkerställer Internets funktionsduglighet och integritet i hela världen[58]. Denna uppsättning omfattar domännamnssystemet (DNS) och dess hierarkiska och delegerade system av zoner, med början högst upp i hierarkin, med rotzonen och de tretton DNS-rotservrar[59] som World Wide Web är beroende av. Kommissionen avser att ta fram en **beredskapsplan, med stöd av EU-medel, för att hantera extrema scenarier som påverkar det globala DNS-rotsystemets integritet och tillgänglighet**. Den kommer att samarbeta med Enisa, medlemsstaterna, EU:s två DNS-rotserveroperatörer[60] och flerpartssamhället för att bedöma dessa operatörers roll när det gäller att garantera att internet förblir globalt tillgängligt under alla omständigheter.

För att en kund ska få tillgång till en resurs under ett visst domännamn på internet måste kundens förfrågan (vanligtvis rörande en webbadress, en s.k. URL) översättas till en IP-adress (av ett program kallat ”resolver” som gör en ”uppslagning”) genom hänvisning till DNS-namnservrar. Människor och organisationer i EU förlitar sig dock i allt högre grad på ett fåtal offentliga DNS-resolvrar som drivs av enheter utanför EU. En sådan konsolidering av DNS-uppslagningar i händerna på ett fåtal företag[61]gör uppslagningsprocessen sårbar i händelse av betydande händelser som påverkar en stor leverantör, och gör det svårare för

[54] I rådets slutsatser efterlyses övergripande åtgärder avseende cybersäkerhet för uppkopplade enheter, 13629/20, 2 december 2020.
[55]Direktiv 2014/53/EU
[56] Följer den FN-föreskrift som antogs i juni 2020, http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
[57] Översyn av de nuvarande allmänna produktsäkerhetsbestämmelserna (direktiv 2001/95/EG), förslag till anpassade regler planeras också om tillverkares ansvar på det digitala området inom ramen för EU:s regelverk för skadeståndsansvar.
[58]”Den offentliga kärnan av ett öppet internet, nämligen dess huvudsakliga protokoll och infrastruktur utgör globala allmänna nyttigheter, ger internet dess viktiga funktioner som en helhet och underbygger dess normala funktion. Enisa bör stödja säkerheten för den offentliga kärnan av ett öppet internet och stabiliteten för dess funktionssätt och bland annat, men inte begränsat till, nyckelprotokollen (framför allt DNS, BGP och IPv6), driften av domännamnssystemet (till exempel driften av alla toppdomäner) och driften av rotzonen.” Skäl 23 i cybersäkerhetsakten.
[59]https://www.iana.org/domains/root/servers
[60]De i.root-servrar som drivs av Netnod i Sverige och k.root-servrar som drivs av RIPE NCC i Nederländerna.
[61]Konsolidering på DNS-resolver-marknaden – Hur omfattande? Hur snabb? Hur farlig? (), Tecken på minskad Internet-entropi – brist på redundans i större webbplatsers och tjänsters DNS-uppslagningar ( )

EU:s myndigheter att hantera eventuella fientliga cyberattacker och stora geopolitiska och tekniska incidenter[62].

För att minska säkerhetsproblemen kopplade till en marknadskoncentrationen kommer kommissionen att uppmuntra berörda aktörer, däribland företagen i EU, internetleverantörerna och leverantörerna av webbläsare, att anta en strategi för diversifiering av DNS-uppslagningarna. Kommissionen har också för avsikt att bidra till en säker internetkonnektivitet genom att stödja utvecklingen av en publik **DNS-resolver-tjänst på EU-nivå.** Genom det här ”DNS4EU”-initiativet kommer det att erbjudas en alternativ tjänst, på EU-nivå, för tillgång till det globala internet. DNS4EU kommer att vara transparent, följa de senaste standarderna och reglerna för säkerhet, dataskydd och integritetsskydd, inbyggt och som standard, och utgöra en del av industrialliansen för data och molntjänster (*European Industrial Alliance for Data and Cloud*)[63].

Kommissionen kommer också, i samarbete med medlemsstaterna och industrin, att **påskynda införandet av centrala internetstandarder som inkluderar IPv6**[64] **och väletablerade internetsäkerhetsstandarder och god säkerhetspraxis för DNS, dirigering och e-post**[65], utan att för den skull utesluta lagstiftningsåtgärder såsom en europeisk tidsfristklausul för IPv4, för att styra marknaden, om det inte görs tillräckliga framsteg i riktning mot antagandet av dem. EU bör (t.ex. inom ramen för EU-Afrika-strategin[66]) främja genomförandet av dessa standarder i partnerländerna som ett sätt att stödja utvecklingen av ett globalt och öppet internet och motverka slutna och kontrollbaserade internetmodeller. Slutligen kommer kommissionen att överväga behovet av en mekanism för mer systematisk övervakning och insamling av aggregerade uppgifter om internettrafik och för rådgivning om eventuella störningar[67].

1.7. Ökad närvaro i den tekniska försörjningskedjan

EU har, med det ekonomiska stöd som EU planerar till cybersäker digital omvandling under den fleråriga budgetramen 2021–2027, en unik möjlighet att samla sina tillgångar för att driva på sin industristrategi[68] och sin ledarroll inom digital teknik och cybersäkerhet i hela den digitala leveranskedjan (inklusive data och molntjänster, nästa generations processorteknik, ultrasäker konnektivitet och 6G-nät), i linje med sina värderingar och prioriteringar. Insatser från den offentliga sektorn bör bygga på de verktyg som tillhandahålls genom EU:s regelverk för offentlig upphandling och viktiga projekt av gemensamt europeiskt intresse. Utöver detta kan den frigöra privata investeringar genom offentlig-privata partnerskap (bland annat genom att bygga vidare på erfarenheterna från det avtalsbaserade offentlig-privata partnerskapet om

[62] Det finns också belägg för att DNS-data kan användas för profileringsändamål, vilket har inverkan på rättigheter avseende integritet och uppgiftsskydd.

[63] Gemensam förklaring om inrättandet av nästa generations molntjänster för företag och den offentliga sektorn i EU, https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64]Införandet av IPv6 har nu kommit längre i och med den kraftiga uttömningen av utbudet och ökningen av kostnaderna för IPv4-adresser. Införandet av IPv6 sker dock ojämnt i EU.

[65]Sådana standarder omfattar DNSSEC, HTTPS, DNS over HTTPS (DoH), DNS over TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE samt normer och god praxis för dirigering, t.ex. Mutually Agreed Norms for Routing Security (MANRS).

[66]Gemensamt meddelande - Mot en övergripande strategi för Afrika, JOIN(2020) 4 final, 9.3.2020.

[67] Ett sådant ”Internetobservatorium” skulle kunna ingå i verksamheten vid Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning, Förslag till förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum, COM(2018) 630 final.

[68]Meddelande om en ny industristrategi för EU, COM(2020) 102 final.

cybersäkerhet och dess genomförande via Europeiska cybersäkerhetsorganisationen), riskkapital till stöd för små och medelstora företag eller industriallianser och strategier för teknisk kapacitet.

Särskild uppmärksamhet kommer också att ägnas åt instrumentet för tekniskt stöd[69] och bästa möjliga användning av de senaste cybersäkerhetsverktygen i små och medelstora företag – särskilt de som inte omfattas av det reviderade NIS-direktivet – bland annat genom särskild verksamhet inom ramen för de digitala innovationsknutpunkterna i programmet för ett digitalt Europa. Målet är att generera liknande investeringar från medlemsstaterna, som ska matchas av industrin inom ramen för ett partnerskap som samförvaltas med medlemsstaterna i de föreslagna **Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum (CCCN)**. CCCN bör spela en nyckelroll, med bidrag från industrin och den akademiska världen, när det gäller att utveckla EU:s tekniska suveränitet inom cybersäkerhet, bygga upp kapacitet för att säkra känslig infrastruktur såsom 5G och minska beroendet av andra delar av världen för att få tillgång till den viktigaste tekniken.

Kommissionen har för avsikt att, eventuellt tillsammans med CCCN, stödja utvecklingen av ett särskilt mastersprogram i cybersäkerhet och bidra till en gemensam europeisk färdplan för forskning och innovation om cybersäkerhet efter 2020. Investeringarna via CCCN skulle också bygga vidare på samarbetet kring forskning och utveckling som bedrivs av nätverken av kompetenscentrum för cybersäkerhet, och sammanföra Europas bästa forskarlag med näringslivet för att utforma och genomföra gemensamma forskningsagendor, i linje med Europeiska cybersäkerhetsorganisationens färdplan[70]. Kommissionen kommer att fortsätta att förlita sig på det forskningsarbete som utförs av Enisa och Europol och kommer också att fortsätta att, som en del av Horisont Europa, stödja enskilda internetinnovatörer som utvecklar integritetsfrämjande och säker kommunikationsteknik baserad på programvara och hårdvara med öppen källkod, såsom för närvarande sker inom ramen för initiativet nästa generations internet.

1.8. En cyberkvalificerad arbetskraft i EU

EU:s insatser för att öka arbetskraftens kompetens, utveckla, locka och behålla de bästa talangerna inom cybersäkerhet och investera i forskning och innovation i världsklass utgör en viktig del av skyddet mot cyberhot i allmänhet. Detta område har stor potential. Därför måste särskild uppmärksamhet ägnas åt att utveckla, locka och behålla mer diversifierade begåvningar. Den reviderade handlingsplanen för digital utbildning kommer att öka medvetenheten om cybersäkerhet bland enskilda personer, särskilt barn och ungdomar, och organisationer, särskilt små och medelstora företag[71]. Det kommer också att uppmuntra kvinnors deltagande i utbildningar inom naturvetenskap, teknik, ingenjörsvetenskap och matematik, och kompetenshöjning och omskolning av digitala färdigheter inom IKT-jobb. Dessutom kommer kommissionen, tillsammans med EU:s immaterialrättsmyndighet vid Europol, Enisa, medlemsstaterna och den privata sektorn, att utveckla verktyg för att öka medvetenheten och riktad vägledning som kommer att öka resiliensen hos företagen i EU **mot stöld av immateriella rättigheter med användning av cyberteknik**[72].

[69] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:0409:FIN .
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[72] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2187

Utbildning – inbegripet yrkesutbildning, ökning av medvetenheten och övningar – bör också ytterligare öka kompetensen inom cybersäkerhet och cyberförsvar på EU-nivå. I detta syfte bör berörda EU-aktörer såsom Enisa, Europeiska försvarsbyrån (EDA) och Europeiska säkerhets- och försvarsakademin (Esfa)[73] eftersträva synergier mellan sina respektive verksamheter.

Strategiska initiativ

EU bör säkerställa följande:

- Antagande av det reviderade NIS-direktivet.
- Lagstiftningsåtgärder för ett säkert sakernas internet.
- Genom CCCN-investeringar i cybersäkerhet (särskilt genom programmet för ett digitalt Europa, Horisont Europa och återhämtningsfaciliteten) för att nå upp till 4,5 miljarder euro i offentliga och privata investeringar under perioden 2021–2027.
- Ett EU-nätverk av AI-baserade säkerhetscentrum och en ultrasäker kommunikationsinfrastruktur som utnyttjar kvantteknik.
- Utbredd användning av cybersäkerhetsteknik genom särskilt stöd till små och medelstora företag inom ramen för de digitala innovationsknutpunkterna.
- Utveckling av en DNS-resolver-tjänst på EU-nivå som ett säkert och öppet alternativ för EU:s medborgare, företag och offentliga förvaltningar att få tillgång till internet.
- Slutförande av genomförandet av verktygslådan för 5G senast andra kvartalet 2021 (se bilagan).

2. Operativ kapacitet för att förebygga, motverka och bemöta

Cyberincidenter kan orsaka enorma skador, oavsett om de är oavsiktliga eller om det rör sig om avsiktliga handlingar från brottslingar, statliga och andra icke-statliga aktörer. Deras omfattning och komplexitet, ofta utnyttjande av tredjepartstjänster, hårdvara och programvara för att komma åt slutmålet, gör det svårt att hantera den samlade hotmiljön i EU utan systematiskt och omfattande informationsutbyte och samarbete kring en gemensam åtgärd. EU har som mål att **genom full tillämpning av regleringsverktyg, mobilisering och samarbete** stödja medlemsstaterna i försvaret av sina medborgare, sina ekonomiska intressen och nationella säkerhetsintressen, med full respekt för grundläggande rättigheter och friheter och rättsstatsprincipen. Flera grupper, bestående av nätverk, EU:s institutioner, organ och byråer samt medlemsstaternas myndigheter, ansvarar för att förebygga, avskräcka, motverka och bemöta cyberhot med hjälp av sina respektive instrument och initiativ[74]. Dessa grupper

[73]Genom plattformen för utbildning, övning och utvärdering på cyberområdet (ETEE).

[74]Inklusive stöd från Europeiska unionens cybersäkerhetsbyrå (Enisa) till operativt samarbete och krishantering, CSIRT-nätverket, nätverket med cyberkriskontaktorganisationer (CyCLONe, som ska bli EU-CyCLONe enligt förslaget i det reviderade NIS-direktivet), NIS-samarbetsgruppen, ”rescEU”, arbetsgruppen mot cyberbrottslighet (*Joint Cybercrime Action Task Force*) vid Europol och beredskapsprotokollet för EU:s brottsbekämpningsinsatser (*Law Enforcement Emergency Response Protocol*), EU:s underrättelse- och lägescentral (EU Intcen) och verktygslådan för cyberdiplomati, den gemensamma kapaciteten för underrättelseanalys (SIAC), cyberprojekten inom ramen för det permanenta strukturerade samarbetet (Pesco),

omfattar följande: i) NIS-myndigheter, till exempel CSIRT, och katastrofinsatser. ii) Brottsbekämpande och rättsliga myndigheter. iii) Cyberdiplomati. iv) It-försvar.

2.1. En gemensam cyberenhet

En gemensam cyberenhet skulle fungera som en virtuell och fysisk plattform för samarbete mellan olika cybersäkerhetsgrupper i EU, med fokus på operativ och teknisk samordning mot större gränsöverskridande cyberincidenter och cyberhot**.**

Den gemensamma cyberenheten skulle vara ett viktigt steg framåt mot fullbordandet av **den europeiska ramen för hantering av cyberkriser**. I enlighet med kommissionsordförandens politiska riktlinjer[75] bör enheten göra det möjligt för medlemsstaterna och EU:s institutioner, organ och byråer att fullt ut utnyttja befintliga strukturer och resurser och främja ett ”**behovsenligt**” tankesätt. Den skulle göra det möjligt att konsolidera de framsteg som hittills gjorts i genomförandet av 2017 års rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (”samordningsplanen”)[76]. Det skulle också erbjuda tillfälle att ytterligare stärka samarbetet kring samordningsplanen och utnyttja de framsteg som gjorts, särskilt inom NIS-samarbetsgruppen och CyCLONe-nätverket.

Detta skulle kunna åtgärda **två huvudsakliga luckor** som för närvarande ökar sårbarheten och skapar ineffektivitet vid hanteringen av gränsöverskridande hot och incidenter som drabbar unionen. För det första har de civila, diplomatiska, brottsbekämpande och försvarsrelaterade cybersäkerhets**grupperna** ännu inte något gemensamt utrymme för att främja strukturerat samarbete och underlätta operativt och tekniskt samarbete. För det andra har de relevanta berörda aktörerna på cybersäkerhetsområdet ännu inte kunnat utnyttja den fulla **potentialen** hos det operativa samarbetet och det ömsesidiga biståndet inom de befintliga nätverken och grupperna. Detta inbegriper avsaknaden av en plattform som möjliggör operativt samarbete med den privata sektorn. Enheten skulle förbättra och påskynda samordningen och göra det möjligt för EU att hantera och reagera på storskaliga cyberincidenter och cyberkriser.

Den gemensamma cyberenheten skulle inte utgöra ett ytterligare fristående organ, inte heller påverka de nationella cybersäkerhetsmyndigheternas eller EU-deltagarnas befogenheter. Den skulle snarare fungera som en säkerhetsmekanism där deltagarna kan dra nytta av varandras stöd och expertis, särskilt om olika cybergrupper måste ha ett nära samarbete. Samtidigt visar den senaste tidens händelser att EU måste höja sin ambitionsnivå och beredskap att ställas inför hotbilden inom cyberområdet och verkligheten. Som en del av bidraget till den gemensamma cyberenheten är EU-aktörerna (kommissionen och EU:s byråer och organ) därför beredda att avsevärt öka sina resurser och sin kapacitet för att höja nivån på sin beredskap och resiliens.

Den gemensamma cyberenheten skulle uppfylla tre huvudsakliga mål. För det första skulle den säkerställa **beredskap** i alla cybersäkerhetsgrupper. För det andra skulle den via informationsutbyte tillhandahålla en kontinuerlig kollektiv situations**medvetenhet**. För det tredje skulle den stärka den samordnade **responsen** och återhämtning. För att åstadkomma

---

särskilt ”snabbinsatsteamen och det ömsesidiga biståndet på området för cybersäkerhet” (*Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity*, CRRT).

[75] *En ambitiösare union - Min agenda för Europa*, Politiska riktlinjer för nästa Europeiska kommission 2019–2024 av kandidaten till befattningen som Europeiska kommissionens ordförande Ursula von der Leyen.

[76] Rekommendation om en samordningsplan C(2017) 6100 final av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser.

detta skulle enheten bygga vidare på väldefinierade **block och mål**, såsom att garantera **säker och snabb informationsdelning**, förbättra **samarbetet** mellan parterna, inklusive interaktion mellan medlemsstaterna och relevanta EU-enheter, upprätta strukturerade **partnerskap med en betrodd industribas** och underlätta en samordnad strategi för **samarbete med externa parter**. För att åstadkomma detta, vilket skulle baseras på enhetens kapacitet på nationell nivå och EU-nivå, skulle enheten kunna underlätta utvecklingen av en samarbetsram.

För att den gemensamma cyberenheten ska bli navet i EU:s operativa samarbete kring cybersäkerhet kommer kommissionen att arbeta med medlemsstaterna och EU:s relevanta institutioner, organ och byråer, bland annat Enisa, Cert-EU och Europol, för att främja ett **stegvis ökande och inkluderande tillvägagångssätt**, varvid alla inblandades befogenheter och mandat till fullo beaktas. I enlighet med detta tillvägagångssätt skulle enheten kunna bidra till ytterligare samarbete mellan olika aktörer i en viss cybergrupp, om dessa aktörer anser det nödvändigt.

Fyra huvudsakliga steg föreslås för att genomföra den gemensamma cyberenheten i praktiken:

- *Fastställa*, genom att kartlägga tillgänglig kapacitet på nationell nivå och EU-nivå,
- *Utarbeta*, genom att inrätta en ram för strukturerat samarbete och bistånd.
- *Införa*, genom att genomföra ramen varvid resurser som tillhandahålls av deltagarna utnyttjas så att den gemensamma cyberenheten kan tas i drift.
- *Utöka*, genom att stärka kapacitet till samordnade insatser med bidrag från industrin och partner.

På grundval av resultatet av samrådet med medlemsstaterna, EU:s institutioner, organ och byråer[77], kommer kommissionen med deltagande av den höge representanten, i enlighet med dennas kompetens, senast i februari 2021 lägga fram processen, etappmålen och tidsplanen för att **fastställa, utarbeta, införa och utöka den gemensamma cyberenheten.**

2.2. Ta itu med cyberbrottsligheten

Vårt beroende av onlineverktyg har ökat attackytan för cyberbrottslingar exponentiellt och lett till en situation där utredningar av nästan alla typer av brott har ett digitalt inslag. Dessutom hotas centrala delar av vårt samhälle av cyberaktörer och av dem som använder cyberverktyg för att planera och genomföra olagliga handlingar. Det finns därför nära kopplingar till EU:s övergripande säkerhetspolitik, vilket återspeglas i cyberdelarna av strategin för EU:s säkerhetsunion från 2020 inom ramen för denna och i EU:s agenda för terrorismbekämpning[78].

En effektiv hantering av cyberbrottslighet är en nyckelfaktor för att säkerställa cybersäkerheten: motverkan kan inte uppnås enbart genom resiliens, utan kräver även identifiering och lagföring av de som brutit mot lagen. Det är därför viktigt att främja samarbete och utbyte mellan cybersäkerhetsaktörer och de brottsbekämpande organen På EU-

[77]Samrådet med medlemsstaterna (bland annat Blue OLEx20-övningen där cheferna för de nationella cybersäkerhetsmyndigheterna samlas) samt EU:s institutioner, organ och byråer ägde rum juli-november 2020.
[78]*Communication: A Counter-Terrorism Agenda for the EU - Anticip, Prevent, Protect, Respond*, 9.12.2020, COM (2020) 795 final (ej översatt till svenska).

nivå har Europol och Enisa därför redan byggt upp ett starkt samarbete där de har anordnat gemensamma konferenser och workshoppar och lämnat gemensamma rapporter till kommissionen, medlemsstaterna och andra berörda parter om cybersäkerhetshot och tekniska utmaningar. Kommissionen kommer att fortsätta stödja denna integrerade strategi för att säkerställa en enhetlig och effektiv respons, baserad på en heltäckande informationsbild.

Som en viktig del av denna respons måste EU och de nationella myndigheterna utöka och förbättra de brottsbekämpande organens kapacitet att utreda cyberbrottslighet, fullt respektera de grundläggande rättigheterna och eftersträva den balans som krävs mellan olika rättigheter och intressen. EU bör kunna bekämpa cyberbrottslighet med hjälp av lagstiftning som har genomförts fullt ut och är ändamålsenlig, med särskild tyngdpunkt på bekämpning av sexuella övergrepp mot barn på internet, och på digitala utredningar, inbegripet brottslighet på det s.k. darknet. De brottsbekämpande organen måste vara fullt utrustade för digitala utredningar. Kommissionen kommer därför att lägga fram en handlingsplan för att förbättra de brottsbekämpande organens digitala kapacitet genom att förse dem med nödvändiga färdigheter och verktyg. Dessutom kommer Europol att vidareutveckla sin roll som ett expertcentrum för att stödja nationella brottsbekämpande myndigheter som bekämpar brottslighet som möjliggörs av cyberteknik och cyberberoende brottslighet, och bidra till fastställandet av gemensamma kriminaltekniska standarder (genom Europols innovationslabb och innovationsknutpunkt). Alla dessa verksamheter kräver lämpligt anammande av medlemsstaterna, som uppmuntras att använda sig av de nationella programmen inom fonden för inre säkerhet och att föreslå projekt vid inbjudningar att lämna förslag som en del av den tematiska faciliteten.

Kommissionen kommer att använda alla tillämpliga medel, inklusive överträdelseförfaranden, för att se till att 2013 års direktiv om angrepp mot informationssystem[79] införlivas och genomförs fullt ut, inbegripet tillhandahållande från medlemsstaterna av statistik. Den kommer att bättre kunna förhindra missbruk av domännamn, och när så är lämpligt även missbruk av domännamn i syfte att distribuera olagligt innehåll, och eftersträva tillgång till korrekta registreringsuppgifter genom att även fortsättningsvis ha kontakt med ICANN (*Internet Corporation for Assigned Names and Numbers*) och andra intressenter i systemet för förvaltning av internet, särskilt genom arbetsgruppen för allmän säkerhet (*Public Safety Working Group*) inom ICANN:s mellanstatliga rådgivande kommitté. Enligt förslaget i det reviderade NIS-direktivet ska därför korrekta och fullständiga databaser över domännamn och registreringsuppgifter, så kallade WHOIS-data, bevaras och laglig tillgång ges till sådana uppgifter som är nödvändiga för att säkerställa DNS-systemets säkerhet, stabilitet och resiliens.

Kommissionen kommer också fortsätta att arbeta för att tillhandahålla lämpliga kanaler för och klargöra de bestämmelser som reglerar gränsöverskridande tillgång till elektroniska bevis för brottsutredningar (som behövs i 85 % av utredningarna, varav 65 % av de totala ansökningarna går till leverantörer som är baserade i en annan jurisdiktion), genom att underlätta antagandet, och det efterföljande genomförandet, av paketet om e-bevisning och praktiska åtgärder[80]. Europaparlamentet och rådet bör snabbt anta förslagen om elektroniska

[79]Direktiv 2013/40/EU om angrepp mot informationssystem.

[80]COM(2018) 225 och 226, C(2020) 2779 final. Framför allt fick Sirius-projektet nyligen ytterligare finansiering inom ramen för partnerskapsinstrumentet för att förbättra kanalerna för att få laglig gränsöverskridande tillgång till elektroniska bevis för brottsutredningar (som behövs i 85 % av utredningarna av

bevis för att förse polisen med effektiva verktyg. Elektroniska bevis måste vara läsbara, och därför kommer kommissionen att fortsätta arbetet med stödet till brottsbekämpningskapaciteten på området för digitala utredningar, inbegripet hantering av kryptering när man stöter på brottsutredningar, samtidigt som dess funktion att skydda de grundläggande rättigheterna och cybersäkerheten bevaras fullt ut.

2.3. EU:s verktygslåda för cyberdiplomati

EU har använt sin **verktygslåda för cyberdiplomati**[81] för att förebygga, avskräcka, motverka och bemöta skadlig cyberverksamhet. Efter införandet av den rättsliga ramen för riktade restriktiva åtgärder mot cyberattacker i maj 2019[82] förtecknade EU sex personer och tre enheter som bär ansvaret för eller har deltagit i cyberattacker som påverkat EU och dess medlemsstater inom ramen för systemet i juli 2020[83]. Ytterligare två personer och ett organ lades till i förteckningen i oktober 2020[84]. Skadlig cyberverksamhet, inbegripet långsamt verkande, bör hanteras genom en effektiv och övergripande gemensam diplomatisk respons från EU, med användande av alla de åtgärder som finns tillgängliga på EU-nivå.

En snabb och effektiv gemensam diplomatisk respons från EU kräver en solid gemensam situationsmedvetenhet och förmåga att snabbt utarbeta en gemensam EU-ståndpunkt. Unionens höga representant för utrikes frågor och säkerhetspolitik kommer att uppmuntra och underlätta inrättandet av medlemsstaternas arbetsgrupp för cyberunderrättelser (*Member States' EU cyber intelligence working group*) inom EU:s underrättelse- och lägescentral (EU Intcen) för att främja strategiskt underrättelsesamarbete om cyberhot och cyberaktiviteter. Detta arbete kommer att ytterligare bidra till EU:s situationsmedvetenhet och beslutsfattande om en gemensam diplomatisk respons. Arbetsgruppen ska samarbeta med befintliga strukturer[85], vid behov även sådana som täcker det bredare hotet från hybridinblandning och utländsk inblandning, för att samla in underrättelser och bedöma situationsmedvetenheten.

För att stärka sin förmåga att förebygga, avskräcka, motverka och bemöta skadligt beteende i cyberrymden kommer den höga representanten, med deltagande av kommissionen i enlighet med dess befogenheter, lägga fram ett förslag om att EU ytterligare ska definiera sin **cyberavskräckningskapacitet**. Med utgångspunkt i det arbete som hittills utförts inom

---

allvarliga brott, och 65 % av det totala antalet ansökningar går till leverantörer som är baserade i en annan jurisdiktion) och fastställande av kompatibla regler på internationell nivå.

[81] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] Rådets beslut (Gusp) 2019/797 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 129 I, 17.5.2019, s. 13), och rådets förordning (EU) 2019/796 den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 129I, 17.5.2019, s. 1).

[83] Rådets beslut (Gusp) 2020/1127 av den 30 juli 2020 om ändring av beslut (Gusp) 2019/797 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (ST/9564/2020/INIT) (EUT L 246, 30.7.2020, s. 12), och rådets genomförandeförordning (EU) 2020/1125 av den 30 juli 2020 om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (ST/9568/2020/INIT) (EUT L 246, 30.7.2020, s. 4).

[84] Rådets beslut (Gusp) 2020/1537 av den 22 oktober 2020 om ändring av beslut (Gusp) 2019/797 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 351I, 22.10.2020, s. 5). och rådets genomförandeförordning (EU) 2020/1536 av den 22 oktober 2020 om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 351I, 22.10.2020, s. 1).

[85] Såsom EU:s gemensamma kapacitet för underrättelseanalys (SIAC) och, vid behov, de relevanta projekt som inrättats inom ramen för Pesco, samt 2018 års system för snabb varning som inrättats för att stödja EU:s övergripande strategi för att bekämpa desinformation.

ramen för verktygslådan för cyberdiplomati bör kapaciteten bidra till staters ansvarsfulla agerande och samarbete i cyberrymden, och bör ge särskild vägledning när det gäller att motverka de cyberangrepp som har störst inverkan, särskilt de som påverkar vår kritiska infrastruktur, och våra demokratiska institutioner och processer[86], samt attacker på leveranskedjan och cyberbaserade stöld av immateriella rättigheter. I kapaciteten bör det beskrivas hur EU och medlemsstaterna kan utnyttja sina politiska, ekonomiska, diplomatiska, rättsliga och strategiska kommunikationsverktyg mot skadlig cyberverksamhet, samt tas upp hur EU och medlemsstaterna kan förbättra sin kapacitet att hitta de skyldiga till skadlig cyberverksamhet. Dessutom har den höga representanten för avsikt att tillsammans med rådet och kommissionen undersöka **ytterligare åtgärder inom ramen för verktygslådan för cyberdiplomati**, inbegripet möjligheten till ytterligare alternativ för restriktiva åtgärder inklusive genom att undersöka möjligheten till **omröstning med kvalificerad majoritet om uppförande på förteckningen inom det övergripande systemet med sanktioner för att motverka cyberattacker.** Dessutom bör EU göra ytterligare ansträngningar för att stärka samarbetet med internationella partner, däribland Nato, för att främja den gemensamma förståelsen av hotbilden, utveckla samarbetsmekanismer och identifiera en gemensam diplomatisk respons.

Den höga representanten kommer också, med kommissionens medverkan, att föreslå en uppdatering av **riktlinjerna för genomförandet av verktygslådan för cyberdiplomati[87]**, bland annat för att öka effektiviteten i beslutsprocessen, och fortsätter regelbundet att organisera övningar och göra utvärderingar av verktygslådan. Dessutom bör EU ytterligare **integrera verktygslådan för cyberdiplomati i EU:s krishanteringsmekanismer**, eftersträva synergier med insatser för att motverka hybridhot, desinformation och utländsk inblandning inom den gemensamma ramen för att motverka hybridhot[88] och den europeiska handlingsplanen för demokrati. I detta sammanhang bör EU reflektera över samspelet mellan verktygslådan för cyberdiplomati och en eventuell användning av artikel 42.7 i EU-fördraget och artikel 222 i EUF-fördraget[89].

2.4. Stärkt kapacitet i cyberförsvaret

EU och medlemsstaterna behöver stärka sin kapacitet att förebygga och motverka cyberhot i linje med EU:s ambitionsnivå enligt EU:s globala strategi från 2016[90]. I detta syfte kommer den höga representanten, i samarbete med kommissionen, att lägga fram en **översyn av ramen för EU:s politik för it-försvar** för att ytterligare förbättra samordningen och samarbetet mellan EU[91]-aktörerna samt med och mellan medlemsstaterna, bland annat när det gäller uppdrag och insatser inom ramen för den gemensamma säkerhets- och försvarspolitiken (GSFP). Ramen för EU:s politik för it-försvar bör ligga till underlag för den kommande strategiska kompassen[92] och se till att cybersäkerhet och cyberförsvar integreras ytterligare i den bredare säkerhets- och försvarsagendan.

---

[86] Särskilt genom att eftersträva synergier med initiativen inom EU:s handlingsplan för demokrati.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
[89] Klausulen om ömsesidigt försvar respektive solidaritetsklausulen.
[90] Rådets slutsatser om genomförande av EU:s globala strategi på säkerhets- och försvarsområdet (dok. 4149/16).
[91] Särskilt Europeiska utrikestjänsten (EEAS), inbegripet EU:s militära stab (EUMS), Europeiska säkerhets- och försvarsakademin (Esfa), kommissionen och EU-organen, särskilt Europeiska försvarsbyrån (EDA).
[92] Rådets slutsatser om säkerhet och försvar av den 17 juni 2020 (dok. 8910/20).

Under 2018 identifierade EU cyberrymden som ett verksamhetsområde[93]. I det kommande dokumentet **Military Vision and Strategy on Cyberspace as a Domain of Operations** från Europeiska unionens militära kommitté bör ytterligare definieras hur cyberrymden som ett verksamhetsområde möjliggör militära uppdrag och insatser inom GSFP på EU-nivå. Det **militära Cert-nätverket**[94], som för närvarande inrättas av Europeiska försvarsbyrån (EDA), kommer att bidra ytterligare till att avsevärt öka samarbetet mellan medlemsstaterna. För att säkerställa cybersäkerheten i kritisk rymdinfrastruktur under rymdprogrammets ansvar kommer dessutom Europeiska unionens rymdprogrambyrå, i synnerhet Galileos säkerhetsövervakningscentrum, att förstärkas och dess mandat utvidgas till att omfatta andra kritiska tillgångar i rymdprogrammet.

EU och medlemsstaterna bör ytterligare stimulera **utvecklingen av förstklassig cyberförsvarskapacitet** genom olika EU-strategier och -instrument, i synnerhet ramen för EU:s politik för it-försvar, och när så är lämpligt bygga vidare på Europeiska försvarsbyråns arbete. En stark tonvikt måste då läggas på utvecklingen och användningen av nyckelteknik som AI, kryptering och kvantdatorteknik. I enlighet med EU:s prioriteringar för förmågeutveckling från 2018[95] och baserat på rapporten från den första fullständiga samordnade årliga översynen om försvaret (*Coordinated Annual Review on Defence, CARD*)[96] bör EU fortsätta att främja samarbete mellan medlemsstaterna när det gäller **cyberförsvar, forskning, innovation och förmågeutveckling** och i detta sammanhang uppmuntra medlemsstaterna att använda sig av **permanent strukturerat samarbete (*Pesco*)**[97] och **Europeiska försvarsfonden**[98]**.**

Kommissionens kommande **handlingsplan om synergieffekter mellan den civila industrin, försvarsindustrin och rymdindustrin**, som kommer att läggas fram under första kvartalet 2021, kommer att omfatta åtgärder för att ytterligare främja synergieffekter när det gäller program, teknik, innovation och uppstartsföretag, i enlighet med respektive programs styrelseformer[99].

Dessutom bör relevanta synergieffekter och gränssnitt utvecklas mellan cyberförsvarsinitiativ som utvecklas inom andra ramar, inklusive medlemsstaternas cyberrelaterade samverkansprojekt [100] inom ramen för Pesco samt med EU:s cybersäkerhetsstrukturer, för att främja informationsutbyte och ömsesidigt stöd.

---

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

[94] Inrättandet av ett militärt Cert-nätverk på EU-nivå svarar mot ett mål som fastställs i 2018 års ram för EU:s politik för it-försvar och syftar till att främja aktivt samspel och informationsutbyte mellan EU-medlemsstaternas militära incidenthanteringsorganisationer.

[95] I juni 2018 enades medlemsstaterna i Europeiska försvarsbyråns styrelse om att vägleda försvarssamarbetet på EU-nivå.

[96] Godkändes av försvarsministrarna i Europeiska försvarsbyråns styrelse i november 2020. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

[97] Det finns i dagsläget flera cyberrelaterade Pescoprojekt, däribland plattformen för utbyte av information om hantering av cyberhot och cyberincidenter, snabbinsatsteam och ömsesidigt bistånd på området för cybersäkerhet, EU:s cyberakademi och innovationsknutpunkt samt samordningscentrumet för cyber- och informationsområdet (CIDCC).

[98] Inom ramen för Europeiska försvarsfonden har kommissionen redan identifierat möjligheter för forskningssamverkan om cyberförsvar och utvecklingsåtgärder som syftar till att stärka samarbetet, innovationskapaciteten och konkurrenskraften för försvarsindustrin.

[99] T.ex. Horisont Europa, programmet för ett digitalt Europa och Europeiska försvarsfonden.

[100] https://pesco.europa.eu/

Strategiska initiativ

EU bör göra följande:

- Färdigställa den europeiska ramen för hantering av cybersäkerhetskriser och fastställa processen, delmålen och tidsplanen för inrättande av den gemensamma cyberenheten.
- Fortsätta genomförandet av cybersäkerhetsagendan inom ramen för strategin för säkerhetsunionen.
- Uppmuntra och underlätta inrättandet av en medlemsstatsarbetsgrupp för cyberunderrättelseverksamhet inom ramen för EU INTCEN.
- Utveckla EU:s arbete med motverkande åtgärder på cyberområdet för att förebygga, avskräcka, motverka och bemöta fientlig cyberverksamhet.
- Se över cyberförsvarsramen.
- Främja utvecklingen av en ”militär vision och EU-strategi för cyberrymden som operativt område” för militära uppdrag och operationer inom ramen för den gemensamma säkerhets- och försvarspolitiken.
- Stödja synergieffekter mellan civil verksamhet, försvarsindustri och rymdindustri.
- Stärka cybersäkerheten för kritisk rymdinfrastruktur inom rymdprogrammet.

3. ARBETE FÖR EN GLOBAL OCH ÖPPEN CYBERRYMD

EU bör fortsätta sitt arbete med internationella partner för att främja en politisk modell och vision för cyberrymden som bygger på rättsstatsprincipen, mänskliga rättigheter, grundläggande friheter och demokratiska värderingar som bidrar till global social, ekonomisk och politisk utveckling och bidrar till en säkerhetsunion. Det är nödvändigt med internationellt samarbete för att bevara en global, öppen, stabil och säker cyberrymd. EU bör därför fortsätta att arbeta med tredjeländer, internationella organisationer och flerpartsgemenskapen för att utveckla och genomföra en sammanhängande internationell cyberpolitik som präglas av en helhetssyn, med beaktande av att de ekonomiska aspekterna av ny teknik, den inre säkerheten och utrikes-, säkerhets- och försvarspolitiken i allt högre grad hänger samman. Som ett starkt ekonomiskt block och handelsblock som bygger på grundläggande demokratiska värderingar, respekt för rättsstatsprincipen och grundläggande rättigheter har EU också en unik möjlighet att ta ledningen i arbetet med att fastställa och främja internationella normer och standarder.

3.1 EU:s ledarskap när det gäller standarder, normer och ramar på cyberområdet

Intensifiera det internationella standardiseringsarbetet

För att främja och försvara sin vision för cyberrymden på internationell nivå måste EU **intensifiera sitt engagemang och ledarskap i internationella standardiseringsprocesser och öka sin närvaro i internationella och europeiska standardiseringsorgan och andra organisationer för utveckling av standarder** [101]. Den digitala teknikens snabba utveckling

[101] T.ex. Internationella standardiseringsorganisationen (ISO), Internationella elektrotekniska kommissionen (IEC), Internationella teleunionen (ITU), Europeiska standardiseringskommittén(CEN), Europeiska kommittén

innebär att internationella standarder blir allt viktigare som ett komplement till regleringsarbetet på sådana områden som AI, molnteknik, kvantdatorteknik och kvantkommunikation. Internationell standardisering används allt oftare avtredjeländer som vill främja sin egen politiska och ideologiska agenda, som ofta inte motsvarar EU:s värderingar. Det finns också en ökande risk för konkurrerande internationella standardiseringsramar, vilket leder till fragmentering.

De internationella standarderna inom teknik som är ny eller under utveckling och internets kärnarkitektur måste utvecklas i linje med EU:s värderingar för att säkerställa att internet förblir globalt och öppet, att tekniken är människocentrerad och integritetsinriktad och att användningen är lagenlig, säker och etisk. Som ett led i den kommande standardiseringsstrategin bör EU fastställa sina **mål för den internationella standardiseringen** och bedriva ett aktivt och samordnat utåtriktat arbete för att främja dessa mål på internationell nivå. Stärkt samarbete och delade bördor bör sökas med likasinnade partner och europeiska intressenter.

Främja ett ansvarsfullt agerande från stater i cyberrymden

EU fortsätter att tillsammans med internationella partner arbeta för att främja en global, öppen, stabil och säker cyberrymd där **internationell rätt (i synnerhet FN:s stadga)**[102] **iakttas**och **frivilliga icke-bindande normer och regler följs och stater agerar på ett ansvarsfullt sätt**[103]. I och med att effektiviteten försämrats i de multilaterala diskussionerna om internationell säkerhet i cyberrymden måste EU och medlemsstaterna inta en mer proaktiv hållning i diskussionerna i FN och andra berörda internationella forum. Det är EU som är bäst lämpat att **främja, samordna och konsolidera medlemsstaternas ståndpunkter i internationella forum** och man bör **utarbeta en EU-ståndpunkt om tillämpningen av internationell rätt i cyberrymden**. Den höga representanten avser också att tillsammans med medlemsstaterna fortsätta arbetet med sitt inkluderande och konsensusbaserade förslag till politiskt åtagande om ett **handlingsprogram för staters ansvarsfulla agerande i cyberrymden**[104]. Baserat på det befintliga regelverk som godkänts av FN:s generalförsamling[105] erbjuder handlingsprogrammet en plattform för bästa praxis inom FN och föreslår att det ska inrättas en mekanism för att omsätta normerna för staters ansvarsfulla agerande i praktiken och främja kapacitetsuppbyggnad. Den höga representanten vill också stärka och uppmuntra genomförandet av **förtroendeskapande åtgärder** mellan stater, såsom utbyte av bästa praxis på regional och multilateral nivå och bidrag till regionsöverskridande samarbete.

Ökad global konnektivitet bör inte leda till censur, massövervakning, brott mot dataskyddet eller repression mot civilsamhället, den akademiska världen och medborgarna. EU bör

---

för elektroteknisk standardisering(Cenelec), Europeiska institutet för telekommunikationsstandarder (Etsi), Internet Engineering Task Force (IETF), tredje generationens partnerskapsprojekt (3GPP) och Institute of Electrical and Electronics Engineers (IEEE).

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] I enlighet med de relevanta rapporterna från grupperna med regeringsexperter på området för främjande av staters ansvarsfulla agerande i cyberrymden i samband med internationell säkerhet (UNGGE), som godkänts av FN:s generalförsamling, i synnerhet rapporterna från 2015, 2013 och 2010.

[104]https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] I enlighet med de relevanta rapporterna från grupperna med regeringsexperter på området för främjande av staters ansvarsfulla agerande i cyberrymden i samband med internationell säkerhet (UNGGE), som godkänts av FN:s generalförsamling, i synnerhet: rapporterna från 2015, 2013 och 2010.

fortsätta att vara ledande i arbetet med att skydda och främja **mänskliga rättigheter och grundläggande friheter** online. Därför bör EU främja stärkt efterlevnad av internationell lagstiftning och internationella standarder när det gäller mänskliga rättigheter[106]. EU bör också omsätta sin handlingsplan för mänskliga rättigheter och demokrati 2020–2024 i praktiska åtgärder[107] och vidareutveckla sina riktlinjer om yttrandefrihet online och offline[108], **för att öka EU-instrumentens praktiska tillämpning**. EU bör göra uthålliga ansträngningar för att **skydda människorättsförsvarare, civilsamhället och personer inom den akademiska världen som arbetar med sådana frågor som cybersäkerhet, dataskydd, övervakning och censur online**. Därför bör EU utarbeta ytterligare praktiska vägledningar, främja bästa praxis och intensifiera sina insatser för att förhindra missbruk av ny teknik, bland annat genom diplomatiska åtgärder, vid behov, liksom exportkontroll av sådan teknik. EU bör också fortsätta kampen för att skydda samhällets mest utsatta online genom att lägga fram lagstiftning för att bättre skydda barn mot sexuella övergrepp och exploatering samt en strategi för barnens rättigheter.

Konventionen om it-brottslighet (Budapestkonventionen)

EU fortsätter att stödja tredjeländer som vill ansluta sig till **Europarådets konvention om it-brottslighet (Budapestkonventionen)** och arbetet för att sammanställa det **andra tilläggsprotokoll till konventionen** som omfattar åtgärder och skyddsmekanismer för att förbättra det internationella samarbetet mellan brottsbekämpande och rättsliga myndigheter samt mellan myndigheter och tjänsteleverantörer i andra länder, där kommissionen deltar i förhandlingarna på EU:s vägnar[109]. Det aktuella initiativet för ett nytt rättsligt instrument om cyberbrottslighet på FN-nivå riskerar att öka splittringen och försena de mycket välbehövliga nationella reformerna och sammanhängande insatserna för kapacitetsuppbyggnad, vilket potentiellt kan stå i vägen för ett effektivt internationellt samarbete mot cyberbrottslighet. EU ser inget behov av något nytt rättsligt instrument mot cyberbrottslighet på FN-nivå. EU fortsätter att föra **multilaterala samtal om cyberbrottslighet** för att säkerställa respekten för mänskliga rättigheter och grundläggande friheter, genom inkluderande och transparens och med beaktande av tillgänglig sakkunskap, med målet att skapa mervärde för alla.

3.2 Samarbete med partner och flerpartsgemenskapen

EU bör **stärka och utvidga sina cyberdialoger med tredjeländer** för att främja sina värderingar och sin vision för cyberrymden, utbyta bästa praxis och verka för effektivare samarbeten. EU bör också inleda **strukturerade samtal med regionala organisationer**, som t.ex. Afrikanska unionen, Aseans regionala forum, Amerikanska samarbetsorganisationen och Organisationen för säkerhet och samarbete i Europa. Samtidigt bör EU sträva efter att finna gemensamma nämnare, när så är möjligt och lämpligt, med andra partner baserat på gemensamma intressen. EU bör tillsammans med EU-delegationerna och, när så är lämpligt, medlemsstaternas ambassader i hela världen, bilda ett informellt **EU-nätverk för cyberdiplomati**, för att främja EU:s vision för cyberrymden, utbyta information och säkra regelbunden samordning när det gäller utveckling i cyberrymden[110].

---

[106] I synnerhet FN:s stadga och den allmänna förklaringen om de mänskliga rättigheterna.

[107] https://www.consilium.europa.eu/en/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

[109] Rådets beslut av juni 2019 (ref 9116/19).

[110] När så är lämpligt kan detta också främja det informella EU-nätverket för digital diplomati som innefattar medlemsstaternas utrikesministerier.

Baserat på de gemensamma förklaringarna av den 8 juli 2016[111] och den 10 juli 2018[112] bör EU fortsätta att främja **samarbete mellan EU och Nato,** i synnerhet när det gäller cyberförsvar och interoperabilitetskrav. I detta sammanhang bör EU fortsätta att sträva efter att knyta relevanta GSFP-strukturer till Natos federerade uppdragsnätverk (*Federated Mission Networking*), för att möjliggöra interoperabilitet med Nato och partner när så behövs. Samarbete mellan EU och Nato om utbildning och övningar bör undersökas vidare, däribland genom att man försöker hitta synergieffekter mellan Europeiska säkerhets- och försvarsakademin och Natos kunskapscentrum för samordnat cyberförsvar (*Cooperative Cyber Defence Centre of Excellence*).

I enlighet med sina värderingar är EU en stark förespråkare för och främjar en **flerpartsmodell för internetförvaltning**. Ingen enskild enhet, regering eller internationell organisation får försöka få kontroll över internet. EU bör fortsätta engagera sig i olika forum[113] för att stärka samarbetet och säkerställa skyddet av grundläggande rättigheter och friheter, i synnerhet rätten till värdighet, personlig integritet, yttrandefrihet och informationsfrihet. För att främja flerpartssamarbetet om cybersäkerhetsfrågor vill kommissionen och den höga representanten, inom sina respektive behörighetsområden, stärka **de regelbundna och strukturerade kontakterna med berörda parter**, inbegripet den privata sektorn, en akademiska världen och civilsamhället, och understryker att cyberrymdens sammanlänkade karaktär innebär att alla intressenter måste föra en dialog om och anta sitt individuella ansvar för att upprätthålla en global, öppen, stabil och säker cyberrymd. Dessa insatser kommer att ge ett värdefullt underlag för potentiella nyckelåtgärder på EU-nivå.

3.3 Stärka de globala kapaciteterna för att öka den globala resiliensen

För att säkerställa att alla länder kan dra nytta av internets och teknikanvändningens sociala, ekonomiska och politiska vinster fortsätter EU att stödja sina partner för att öka deras cyberresiliens och kapacitet för att utreda och lagföra cyberbrottslighet och hantera cyberhot. För att säkerställa en övergripande samstämmighet bör EU utarbeta en **EU-agenda för extern kapacitetsuppbyggnad på cyberområdet**så att dessa insatser är i linje med EU-riktlinjerna för extern kapacitetsuppbyggnad på cyberområdet[114] och Agenda 2030 för hållbar utveckling[115]. Agendan bör utnyttja sakkunskapen hos medlemsstaterna och berörda EU-institutioner, EU-organ, EU-byråer och EU-initiativ, inklusive EU-nätverket för kapacitetsuppbyggnad på cyberområdet[116], i enlighet med deras respektive mandat. En **EU-nämnd för kapacitetsuppbyggnad på cyberområdet** ska inrättas så att den omfattar EU-institutionernas berörda aktörer och övervaka utvecklingen och identifiera ytterligare synergieffekter och potentiella luckor. EU-nämnden kan även stödja ett stärkt samarbete med medlemsstaterna och med partner från offentlig och privat sektor samt andra berörda internationella organ för att samordna insatserna och förhindra dubbelarbete.

EU:s kapacitetsuppbyggnad på cybersäkerhetsområdet bör även i fortsättning fokusera på västra Balkan och EU:s grannskap samt på partnerländer som genomgår en snabb digital utveckling. EU:s arbete bör stödja utvecklingen av lagstiftning och politik i partnerländerna i

[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/en/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] T.ex. Internet Cooperation for Assigned Names and Numbers (ICANN) och forumet för förvaltning av internet (*Internet Governance Forum, IGF*).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

enlighet med relevanta EU-policyer för cyberdiplomati och standarder. I detta sammanhang bör cybersäkerheten som standard ingå i EU:s kapacitetsuppbyggnadsarbete. Därför bör EU-utarbeta ett utbildningsprogram för sådan EU-personal som ansvarar för genomförandet av EU:s externa kapacitetsuppbyggnad på det digitala området och cyberområdet. EU bör också hjälpa dessa länder att hantera de ökade problemen med skadlig cyberverksamhet som skadar samhällsutvecklingen och de **demokratiska systemens integritet och säkerhet**, i linje med insatserna inom ramen för den europeiska handlingsplanen för demokrati. Ett ömsesidigt lärande mellan EU-medlemsstater och berörda EU-organ och tredjeländer kan vara särskilt fruktbart i detta hänseende.

Inom ramen för den civila GSFP-pakten från 2018[117] kan slutligen civila GSFP-uppdrag också bidra till EU:s bredare insatser mot cybersäkerhetsutmaningar, i synnerhet genom att stärka rättsstatsprincipen inom partnerländerna liksom kapaciteten hos deras brottsbekämpande myndigheter och civila förvaltningar.

Strategiska initiativ

EU bör göra följande:

- Fastställa ett antal mål inom de internationella standardiseringsprocesserna och främja dessa på internationell nivå.
- Främja internationell säkerhet och stabilitet i cyberrymden, i synnerhet genom förslaget i FN från EU och dess medlemsstater om ett handlingsprogram för att främja ansvarsfullt agerande från stater i cyberrymden.
- Erbjuda praktisk vägledning om tillämpningen av mänskliga rättigheter och grundläggande friheter i cyberrymden.
- Bättre skydda barn mot sexuella övergrepp och exploatering, samt strategin för barnens rättigheter.
- Stärka och främja Budapestkonventionen och it-brottslighet, bland annat genom arbetet med det andra tilläggsprotokollet till konventionen.
- Utvidga EU:s cyberdialog med tredjeländer och regionala och internationella organisationer, bland annat genom ett informellt EU-nätverk för cyberdiplomati.
- Stärka kontakterna med flerpartsgemenskapen, framför allt genom regelbundna och strukturerade kontakter med den privata sektorn, den akademiska världen och civilsamhället.
- Föreslå en EU-agenda för extern kapacitetsuppbyggnad på cyberområdet och en EU-nämnd för kapacitetsuppbyggnad på cyberområdet.

III. CYBERSÄKERHET HOS EU:S INSTITUTIONER, ORGAN OCH BYRÅER

På grund av sin höga politiska profil, sina kritiska uppdrag att samordna mycket känsliga frågor och sin roll i förvaltningen av stora summor offentliga medel blir **EU:s institutioner,**

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/en/pdf

organ och byråer regelbundet måltavlor för cyberattacker , i synnerhet cyberspionage. Nivån av cyberresiliens och förmåga att upptäcka och vidta åtgärder mot fientlig cyberverksamhet varierar dock avsevärt mellan dessa enheter i fråga om mogenhetsgrad. Det är därför nödvändigt att förbättra den allmänna cybersäkerhetsnivån genom konsekventa och enhetliga regler.

När det gäller informationssäkerheten har framsteg gjorts mot mer konsekventa **regler för att skydda säkerhetsskyddsklassificerade EU-uppgifter och känsliga uppgifter som inte är säkerhetsskyddsklassificerade**. De säkerhetsskyddsklassificerade informationssystemen har dock fortfarande en begränsad interoperabilitet, vilket förhindrar en sömlös överföring av information mellan olika enheter. Ytterligare framsteg bör göras för att möjliggöra ett interinstitutionellt tillvägagångssätt att hantera säkerhetsskyddsklassificerade EU-uppgifter och känsliga uppgifter som inte är säkerhetsskyddsklassificerade och som också kan fungera som modell för interoperabilitet mellan medlemsstaterna. Ett referensscenario bör också fastställas för att förenkla förfarandena med medlemsstaterna. EU bör även vidareutveckla sin förmåga att på ett säkert sätt kommunicera med relevanta partner och då i möjligaste bygga vidare på befintliga arrangemang och förfaranden.

Såsom aviserades i EU:s strategi för en säkerhetsunion kommer kommissionen därför att lägga fram förslag om **gemensamma bindande regler om informationssäkerhet och gemensamma bindande regler om cybersäkerhet för alla EU:s institutioner, organ och byråer under 2021**, baserat på de pågående interinstitutionella EU-diskussionerna om cybersäkerhet[118].

De nuvarande och framtida trenderna beträffande distansarbete kommer också att kräva ytterligare investeringar i säker utrustning och säkra infrastrukturer och verktyg som gör det möjligt att arbeta med känsliga och säkerhetsklassificerade ärenden på distans.

Den alltmer fientliga miljön av cyberhot och den ökade förekomsten av mer sofistikerade cyberattacker påverkar EU:s institutioner, organ och byråer och skapar ett behov av ökade investeringar för att nå en högre nivå av cybermognad. Ett program för cybermedvetenhet håller på att inrättas för alla EU:s institutioner, organ och byråer för att öka personalens medvetenhet och cyberhygien och främja en gemensam cybersäkerhetskultur.

CERT-EU måste stärkas med en förbättrad finansieringsmekanism för att öka dess förmåga att hjälpa EU:s institutioner, organ och byråer tillämpa de nya cybersäkerhetsreglerna och förbättra deras cyberresiliens. CERT-EU måste också få ett stärkt mandat för att få stabila möjligheter att uppnå dessa mål.

Strategiska initiativ

1. Förordning om informationssäkerhet hos EU:s institutioner, organ och byråer.
2. Förordning om gemensamma cybersäkerhetsregler för EU:s institutioner, organ och byråer.
3. En ny rättslig grund för CERT-EU för att stärka dess mandat och finansiering.

[118] Regelbundna interinstitutionella EU-diskussioner om cybersäkerhet är ett led i de allmänna diskussionerna om den digitala omvandlingens möjligheter och utmaningar för EU-institutionerna.

IV. SLUTSATS

Det samordnade genomförandet av denna strategi kommer att bidra till ett cybersäkert digitalt decennium för EU, till skapandet av en säkerhetsunion och till en stärkt global ställning för EU.

EU bör driva fram standarder och normer för lösningar av världsklass och cybersäkerhetsstandarder för väsentliga tjänster och kritisk infrastruktur samt utvecklingen och tillämpningen av ny teknik. Varje organisation och individ som använder internet är en del av lösningen för att säkerställa en cybersäker digital omställning.

Kommissionen och den höga representanten kommer, baserat på sina respektive befogenheter, att övervaka framstegen inom ramen för denna strategi och utarbeta kriterier för utvärderingen. Rapporter från Enisa och kommissionens regelbundna rapporter om säkerhetsunionen ska användas för denna övervakning. Resultaten kommer att bidra till de kommande målen för det digitala decenniet[119]. Kommissionen och den höga representanten att i enlighet med sina respektive befogenheter att fortsätta sina kontakter med medlemsstaterna för att koppla samman de fyra cybersäkerhetsgemenskaperna i EU, nämligen resiliens för kritisk infrastruktur och den inre marknaden, rättssystem och brottsbekämpning samt cyberdiplomati och cyberförsvar, där så är nödvändigt. Kommissionen och den höga representanten kommer också att fortsätta sina samtal med flerpartsgemenskapen och understryka att alla som använder internet måste göra sitt för att upprätthålla en global, öppen, stabil och säker cyberrymd, där alla kan leva sina digitala liv i säkerhet.

[119] I enlighet med kommissionens arbetsprogram för 2021.

Tillägg: Nästa steg när det gäller cybersäkerheten i 5G-nät.

Baserat på översynen av kommissionens rekommendation om it-säkerhet i 5G-nät[120] bör nästa steg i det samordnade arbetet på EU-nivå fokusera på tre huvudmål och på de viktigaste åtgärderna på kort och medellång sikt i enlighet med tabellen nedan, vilka ska genomföras av medlemsstaternas myndigheter, kommissionen och Enisa.

Den första prioriteringen för nästa fas är att **slutföra genomförandet av verktygslådan på nationell nivå och ta itu med de problem som angavs i lägesrapporten från juli 2020**. I detta sammanhang kan vissa av verktygslådans strategiska åtgärder gagnas av **bättre samordning och ökat informationsutbyte** inom arbetet med nät- och informationssäkerhet, såsom redan anges i lägesrapporten. Detta kan i förlängningen mynna ut i utarbetandet av **bästa praxis eller vägledningar**. När det gäller tekniska åtgärder kan Enisa tillhandahålla ytterligare stöd, baserat på det arbete som de redan har gjort, och utreda vissa frågor mer ingående och **ta fram en heltäckande översikt över alla relevanta riktlinjer avseende 5G-cybersäkerhetskrav för mobiloperatörer**.

För det andra betonade medlemsstaterna betydelsen av att hålla jämna steg med utvecklingen genom att **kontinuerligt övervaka utvecklingen när det gäller teknik, 5G-arkitektur, hot och 5G-användningsområden och -tillämpningar liksom yttre faktorer**, för att kunna **identifiera och ta itu med nya eller kommande risker**. Ett antal aspekter av den inledande riskanalysen bör också granskas närmare, framför allt för att säkerställa att den omfattar hela 5G-ekosystemet, inklusive alla relevanta delar av nätinfrastrukturen och 5G-leveranskedjan. Verktygslådan har utformats som ett flexibelt och anpassningsbart instrument, men om nödvändigt kan åtgärder vidtas på medellång eller lång sikt för att utöka eller ändra den, för att säkerställa att den förblir heltäckande och aktuell.

För det tredje bör man fortsätta att vidta **åtgärder på EU-nivå** för att stödja och komplettera verktygslådans mål och helt integrera dem med relevanta unions- och kommissionsstrategier, i synnerhet för att följa upp de åtgärder inom en mängd områden som kommissionen aviserade i sitt meddelande om verktygslådan av den 29 januari 2020[121] (t.ex. EU-finansiering för säkra 5G-nät, investering i 5G- och post-5G-teknik, handelspolitiska skyddsinstrument och konkurrens för att motverka snedvridning på leveransmarknaden för 5G).

När så är lämpligt bör de ledande aktörerna i början av 2021 anta de detaljerade arrangemangen och delmålen.

Huvudmål 1 Säkerställa mer enhetliga nationella strategier för en effektiv riskreducering i hela EU		
Områden	**De viktigaste åtgärderna på kort och medellång sikt**	**Ledande aktörer**
Medlemsstaternas genomförande av verktygslådan	Slutföra genomförandet av de åtgärder som rekommenderas i verktygslådans slutsatser senast andra kvartalet 2021, med periodisk inventering inom ramen	Medlemsstaternas myndigheter

[120] Kommissionens rapport om konsekvenserna av kommissionens rekommendation 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät.

[121] Kommissionens meddelande COM (2020)50, Säker 5G-utbyggnad i EU – Genomförande av EU:s verktygslåda, 29 januari 2020.

	för arbetet med nät- och informationssäkerhet (*NIS Work Stream*).	
Utbyte av information och bästa praxis om strategiska åtgärder som rör leverantörer	Intensifiera utbytet av information och ta ställning till tänkbar bästa praxis i synnerhet när det gäller följande: - Begränsning av högriskleverantörer (SM03) och åtgärder avseende tillhandahållandet av administrerade tjänster (SM04). - Leveranskedjans säkerhet och resiliens, i synnerhet uppföljning av Berecs undersökning om SM05–SM06.	Medlemsstaternas myndigheter, kommissionen
Kapacitetsuppbyggnad och vägledning om tekniska åtgärder	Göra djupgående tekniska analyser och utveckla gemensamma vägledningar och verktyg, inbegripet följande: - En övergripande och dynamisk matris för säkerhetskontroller och bästa praxis för 5G-säkerhet. Vägledning för att stödja genomförandet av utvalda tekniska åtgärder från verktygslådan'.	Enisa, medlemsstaternas myndigheter
Huvudmål 2 Stöd till kontinuerligt kunskapsutbyte och kapacitetsuppbyggnad		
Områden	**De viktigaste åtgärderna på kort och medellång sikt**	**Ledande aktörer**
Kontinuerligt kunskapsutbyte	Anordna aktiviteter för kunskapsuppbyggnad om teknik och därmed förbundna utmaningar (öppna arkitekturer, 5G-funktioner – t.ex. virtualisering, containerisering, skivning), hotbildens utveckling, faktiska incidenter etc.	Enisa, medlemsstaternas myndigheter, andra berörda parter
Riskbedömning	Uppdatera och utbyta information om uppdaterade nationella riskbedömningar	Medlemsstaternas myndigheter, kommissionen, Enisa
Gemensamma EU-finansierade projekt för att stödja genomförandet av verktygslådan	Lämna finansiellt stöd till projekt som stöder genomförandet av verktygslådan med användning av EU-medel, i synnerhet inom programmet för ett digitalt Europa (t.ex. kapacitetsuppbyggnadsprojekt för nationella myndigheter, testbäddar eller annan avancerad kapacitet).	Medlemsstaternas myndigheter, kommissionen
Samarbete mellan berörda aktörer	Främja samverkan och samarbete mellan nationella myndigheter som hanterar 5G-cybersäkerhet (t.ex. NIS-samarbetsgrupp, cybersäkerhetsmyndigheter, regleringsmyndigheter på teleområdet) och privata aktörer.	Medlemsstaternas myndigheter, kommissionen, Enisa
Huvudmål 3 Främja leveranskedjans resiliens och EU:s övriga strategiska säkerhetsmål		
Områden	**De viktigaste åtgärderna på kort och medellång sikt**	**Ledande aktörer**
Standardisering	Fastställa och genomföra en konkret handlingsplan för att förbättra EU:s representation i standardiseringsorganen som ett led i NIS-undergruppen för standardisering, i syfte att uppnå specifika säkerhetsmål, inklusive främjande av interoperabla gränssnitt för att främja diversifiering av leverantörerna.	Medlemsstaternas myndigheter
Leveranskedjans resiliens	- Göra en ingående analys av 5G-ekosystemet och leveranskedjan för att bättre kunna identifiera och övervaka nyckeltillgångar och potentiellt kritiska	Medlemsstaternas myndigheter, kommissionen

	beroendeförhållanden. - Säkerställa att 5G-marknadens och 5G-leveranskedjans funktioner är förenliga med EU:s handels- och konkurrensregler och mål, i enlighet med kommissionens meddelande av den 29 januari, och att granskning av utländska direktinvesteringar görs i samband med investeringsutveckling som kan påverka 5G-värdekedjan, med beaktande av verktygslådans mål. Övervaka befintliga och förväntade marknadstrender och bedöma möjligheterna på området Open RAN, i synnerhet genom en oberoende studie.	
Certifiering	Inleda förberedelserna för relevanta förslag till certifieringssystem för 5G-nyckelkomponenter och leverantörsprocesser, för att bidra till hanteringen av vissa risker kopplade till teknisk sårbarhet, i enlighet med verktygslådans riskreduceringsplaner.	Kommissionens, Enisa, nationella myndigheter och andra berörda parter
EU-kapacitet och säker utrullning av nät	- Investera i forskning och innovation och kapacitet, i synnerhet genom antagandet av partnerskapet för smarta nät och tjänster. - Införa relevanta säkerhetsvillkor för EU:s finansieringsprogram och finansieringsinstrument (interna och externa), i enlighet med kommissionens meddelande av den 29 januari.	Medlemsstaterna, kommissionen 5G-aktörer
Externa aspekter	Lämna positiva svar till tredjeländer som skulle vilja förstå och potentiellt använda metoderna i den verktygslåda som utvecklats av EU.	Medlemsstaterna, kommissionen Europeiska utrikestjänsten, EU:s delegationer