EUROPEISKA REVISIONSRÄTTEN

SV

2019

Utmaningar för en ändamålsenlig EU politik för cybersäkerhet

Briefingdokument

mars 2019

Om dokumentet:

Syftet med det här briefingdokumentet, som inte är någon granskningsrapport, är att ge en översikt över EU:s komplexa cybersäkerhetspolitiska landskap och identifiera de största utmaningarna för att uppnå ändamålsenliga politiska resultat. Cybersäkerhetspolitik omfattar nät- och informationssäkerhet, it-brottslighet, it-försvar och desinformation. Dokumentet kommer också att fungera som en informationskälla vid eventuellt framtida revisionsarbete på det här området.

Vi har i vår analys utgått från dokumentgranskning av offentligt tillgänglig information i officiella dokument, ståndpunktsdokument och tredjepartsstudier. Fältarbetet utfördes mellan april och september 2018 och utvecklingen fram till december 2018 har beaktats. Vi kompletterade vårt arbete med en enkät bland medlemsstaternas nationella revisionsorgan och intervjuer med viktiga berörda aktörer från EU-institutioner och representanter från den privata sektorn.

De utmaningar som vi identifierade kan grupperas i fyra breda kluster: i) den politiska ramen, ii) finansiering och utgifter, iii) bygga upp cyberresiliens och iv) hantera cyberincidenter ändamålsenligt. Det är absolut nödvändigt att uppnå en högre cybersäkerhetsnivå inom EU. Vi avslutar därför varje kapitel med ett antal idéer för fortsatt reflektion för politiska beslutsfattare, lagstiftare och yrkesverksamma.

Vi tackar för konstruktiv återkoppling från berörda avdelningar vid kommissionen, Europeiska utrikestjänsten, Europeiska unionens råd, Enisa, Europol, den europeiska organisationen för cybersäkerhet och medlemsstaternas nationella revisionsorgan.

Innehållsförteckning

	Punkt
Sammanfattning	I-XIII
Inledning	01-24
Vad är cybersäkerhet?	02-06
Hur allvarligt är problemet?	07-10
EU:s cybersäkerhetsåtgärder	11-24
Politik	13-18
Lagstiftning	19-24
Skapa en politisk och rättslig ram	25-39
Utmaning 1: meningsfull utvärdering och meningsfullt ansvarstagande	26-32
Utmaning 2: hantera brister i EU-lagstiftningen och skillnader i införlivandet	33-39
Finansiering och utgifter	40-64
Utmaning 3: anpassa investeringsnivåerna till målen	41-46
Ökad investering	41-44
Ökad påverkan	45-46
Utmaning 4: en tydlig översikt över EU:s budgetutgifter	47-60
Identifierbara utgifter för cybersäkerhet	50-56
Andra utgifter för cybersäkerhet	57-58
Framtidsutsikter	59-60
Utmaning 5: lämpliga resurser till EU:s byråer	61-64
Skapa ett samhälle präglat av cyberresiliens	65-100
Utmaning 6: stärka styrning och standarder	66-81
Styrning av informationssäkerhet	66-75
Hotbilder och riskbedömningar	76-78
Incitament	79-81

Utmaning 7: öka kompetensen och medvetenheten 82-90

Utveckling av utbildning, kompetens och kapacitet 84-87

Medvetenhet 88-90

Utmaning 8: bättre utbyte och samordning av information 91-100

Samordning mellan EU:s institutioner och medlemsstater 92-96

Samarbete och informationsutbyte med den privata sektorn 97-100

Hantera cyberincidenter ändamålsenligt 101-117

Utmaning 9: ändamålsenlig detektering och hantering 102-111

Detektering och rapportering 102-105

Samordnad hantering 106-111

Utmaning 10: skydda kritisk infrastruktur och kritiska samhällsfunktioner 112-117

Skydda infrastruktur 112-115

Förbättra autonomin 116-117

Avslutande kommentarer 118-121

Bilaga I — Ett komplext landskap i flera skikt med många aktörer

Bilaga II — EU:s utgifter för cybersäkerhet sedan 2014

Bilaga III — Rapporter från revisionsorganen i EU:s medlemsstater

Akronymer och förkortningar

Ordförklaringar

Revisionsrättens team

Sammanfattning

I Tekniken öppnar upp en värld av nya möjligheter där nya produkter och tjänster blir oumbärliga delar av våra dagliga liv. Samtidigt ökar risken för it-brottslighet eller cyberangrepp och de samhälleliga och ekonomiska effekterna av detta fortsätter att öka. EU:s intensifierade insatser sedan 2017 för stärkt cybersäkerhet och digitalt oberoende kommer därmed i rättan tid.

II Det här briefingdokumentet, som inte är någon granskningsrapport och som utgår från offentligt tillgänglig information, syftar till att ge en översikt över ett komplext och oenhetligt politiskt landskap och identifiera de största utmaningarna för att uppnå ändamålsenliga politiska resultat. Dokumentet omfattar EU:s cybersäkerhetspolitik, inbegripet it-brottslighet och it-försvar samt insatser för att bekämpa desinformation. De utmaningar som vi identifierade kan grupperas i fyra breda kluster: i) den politiska och rättsliga ramen, ii) finansiering och utgifter, iii) bygga upp cyberresiliens och iv) hantera cyberincidenter ändamålsenligt. I varje kapitel föreslås ett antal reflektionspunkter kring de utmaningar som presenteras.

Den politiska och rättsliga ramen

III Det är en utmaning att ta fram åtgärder i linje med EU:s strategi för cybersäkerhet och dess brett formulerade mål att bli världens säkraste digitala miljö, eftersom mätbara mål och tillförlitliga data saknas. Resultaten mäts sällan och få politikområden har utvärderats. En viktig utmaning är därför att **säkerställa meningsfullt ansvarstagande och meningsfull utvärdering** genom att övergå till en resultatkultur med inbyggda utvärderingsmetoder.

IV Den rättsliga ramen är fortfarande ofullständig. **Brister i och inkonsekvent införlivande av EU:s lagstiftning** kan göra det svårt att utnyttja lagstiftningen fullt ut.

Finansiering och utgifter

V **Att anpassa investeringsnivåerna till målen** är utmanande: detta inbegriper inte bara att öka investeringarna i cybersäkerhet – vilka i EU har varit låga och fragmenterade – utan också att öka effektiviteten, i synnerhet när det gäller att bättre utnyttja resultaten av forskningsutgifter och säkerställa effektiv målinriktning och finansiering av uppstartsföretag.

VI Det är avgörande att **ha en tydlig översikt över EU:s utgifter** för att EU och medlemsstaterna ska veta vilka brister som måste åtgärdas för att målen ska uppfyllas.

Eftersom det inte finns någon avsatt EU-budget för att finansiera strategin för cybersäkerhet finns det inte någon tydlig bild av vilka pengar som går vart.

VII I en tid av ökade säkerhetsdrivna politiska prioriteringar kan **begränsade resurser för EU:s byråer med cyberrelaterad verksamhet** förhindra att EU:s ambitioner efterlevs. Hantering av den här utmaningen inbegriper att hitta sätt att dra till sig och behålla talanger.

Bygga upp cyberresiliens

VIII Det finns stora svagheter i styrningen av cybersäkerheten i den offentliga och den privata sektorn i hela EU och på internationell nivå. Detta påverkar det globala samfundets förmåga att hantera och begränsa cyberangrepp och undergräver ett konsekvent EU-omfattande tillvägagångssätt. Utmaningen är alltså att **stärka styrningen av cybersäkerheten**.

IX Det är avgörande att **öka kompetensen och medvetenheten** i alla sektorer och på alla samhällsnivåer mot bakgrund av den växande globala kompetensbristen inom cybersäkerhet. För närvarande finns det begränsade EU-omfattande standarder för utbildning, certifiering eller cyberriskbedömningar.

X Grundläggande tillit är avgörande för att stärka den övergripande cyberresiliensen. Kommissionen har själv bedömt att samordningen i allmänhet fortfarande är otillräcklig. Det är fortsättningsvis en utmaning att **förbättra informationsutbytet och samordningen** mellan offentlig och privat sektor.

Hantera cyberincidenter ändamålsenligt

XI De digitala systemen har blivit så komplexa att det är omöjligt att förhindra alla angrepp. Svaret på den här utmaningen är **snabb detektering och hantering**. Dock är cybersäkerhet ännu inte helt integrerat i befintliga samordningsmekanismer för krishantering på EU-nivå, vilket eventuellt begränsar unionens förmåga att hantera storskaliga, gränsöverskridande cyberincidenter.

XII **Skyddet av kritisk infrastruktur och kritiska samhällsfunktioner** är avgörande. Eventuell inblandning i valprocesser och desinformationskampanjer är en kritisk utmaning.

XIII De aktuella utmaningarna med cyberhot mot EU och hela den globala miljön kräver ett kontinuerligt engagemang och att vi orubbligt står fast vid EU:s grundläggande värden.

Inledning

01 Tekniken öppnar upp en värld av nya möjligheter. I takt med att nya produkter och tjänster blir tillgängliga blir de oumbärliga delar av våra dagliga liv. Men med varje ny utveckling ökar vårt beroende av tekniken och därmed också vikten av cybersäkerhet. Ju fler personuppgifter vi lägger ut på internet och ju mer sammanlänkade vi blir, desto sannolikare är det att vi faller offer för någon sorts it-brottslighet eller cyberangrepp.

Vad är cybersäkerhet?

02 Det finns ingen standardiserad, allmänt accepterad definition av cybersäkerhet[1]. I stort handlar det om alla typer av skydd och åtgärder som införs för att försvara informationssystem och deras användare mot obehörig åtkomst, angrepp och skada, för att säkerställa uppgifternas konfidentialitet, integritet och tillgänglighet.

03 Cybersäkerhet inbegriper förebyggande, detektering och hantering av samt återställning efter cyberincidenter. Incidenter kan vara planerade eller oplanerade och till exempel omfatta oavsiktligt röjande av information, angrepp mot företag och kritisk infrastruktur, stöld av personuppgifter och till och med inblandning i demokratiska processer. Allt detta kan ha omfattande skadliga effekter på individer, organisationer och samhällen.

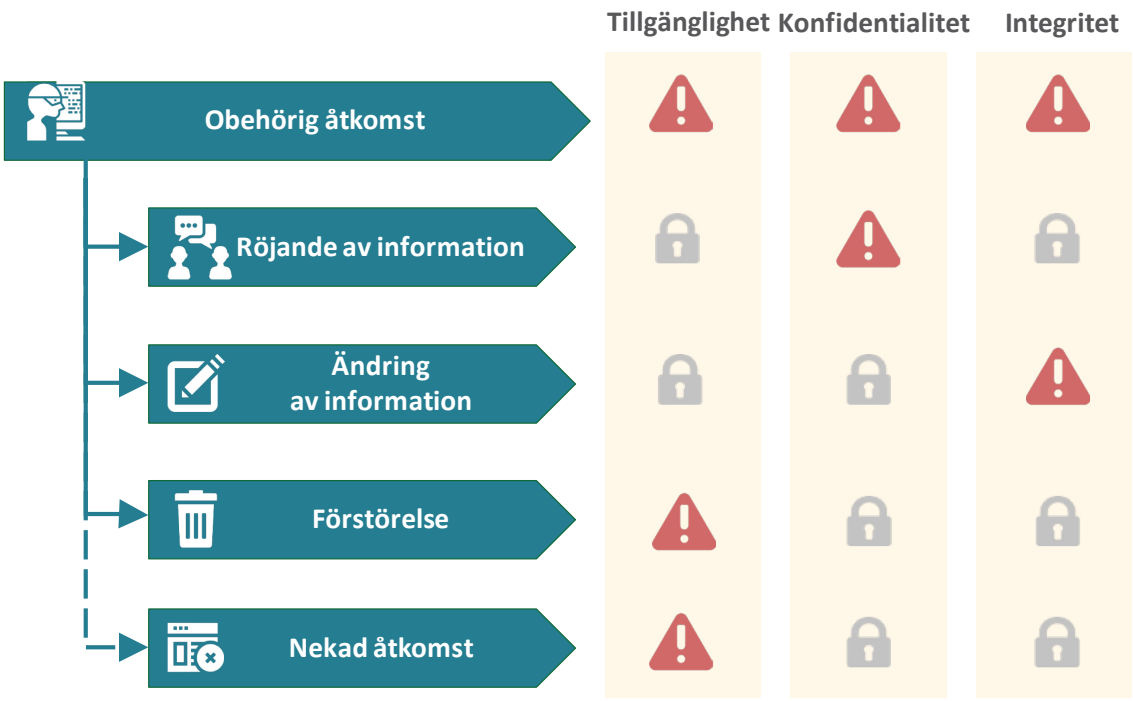
04 Som en term som används i EU-politiska kretsar är cybersäkerhet inte begränsat till nätverks- och informationssäkerhet. Termen omfattar all olaglig verksamhet som inbegriper användning av digital teknik i cyberrymden. Cybersäkerhet kan därför innefatta sådan it-brottslighet som att initiera datorvirusangrepp och genomföra kontantlösa betalningsbedrägerier, men också brottslighet i gränslandet mellan system och innehåll, till exempel spridning av material med sexuella övergrepp mot barn online. Termen kan också omfatta desinformationskampanjer för att påverka onlinedebatten och misstänkt inblandning i val. Dessutom ser Europol ett samband mellan it-brottslighet och terrorism[2].

05 Olika aktörer – inbegripet stater, kriminella grupper och hacktivister – anstiftar cyberincidenter med olika motiv som bakgrund. Konsekvenserna av dessa incidenter är kännbara på nationell, europeisk och till och med global nivå. Men internets immateriella och i stor utsträckning gränslösa natur samt de verktyg och den taktik

som används gör det ofta svårt att identifiera gärningsmannen bakom ett angrepp (det så kallade tillskrivningsproblemet).

06 De olika typerna av cybersäkerhetshot kan klassificeras enligt hur uppgifterna påverkas – röjande, ändring, förstörelse eller nekad åtkomst – eller enligt de grundläggande informationssäkerhetsprinciper som överträds, i enlighet med ***figur 1***. Några exempel på angrepp ges i ***ruta 1***. I takt med att angreppen mot informationssystem blir allt mer sofistikerade blir våra försvarsmekanismer allt mindre effektiva[3].

Figur 1 – Hottyper och de säkerhetsprinciper som riskerar att överträdas



Källa: Revisionsrätten, anpassning av en studie från Europaparlamentet[4]. Hänglås = säkerheten inte påverkad. Utropstecken = säkerheten utsatt för risk.

Ruta 1

Typer av cyberangrepp

Varje gång en ny enhet ansluts till internet eller ansluts till andra enheter ökar den så kallade angreppsytan för cybersäkerhet. Den exponentiella tillväxten av sakernas internet, molnet och stordata samt digitaliseringen av industrin åtföljs av ökad exponering av säkerhetsbrister, vilket gör det möjligt för illvilliga aktörer att komma åt ett större antal offer. De olika typerna av alltmer sofistikerade angrepp gör det väldigt svårt att hålla jämna steg med hoten[5].

Sabotageprogram är utformade för att skada enheter eller nätverk. De kan innefatta virus, trojaner, utpressningstrojaner, maskar, reklamprogram och spionprogram. **Utpressningstrojaner** krypterar data och hindrar användare från att få tillgång till sina filer tills en lösesumma betalas, vanligen i kryptovaluta, eller en åtgärd utförs. Enligt Europol är utpressningstrojaner det slags angrepp som dominerar överlag, och antalet typer av utpressningstrojaner har exploderat under de senaste åren. **DDos-attacker** (samordnade överbelastningsattacker), som gör tjänster eller resurser otillgängliga genom att översvämma dem med fler anrop än de kan hantera, ökar också, och en tredjedel av alla organisationer utsattes för denna typ av angrepp 2017[6].

Användare kan manipuleras till att oavsiktligen utföra en åtgärd eller röja konfidentiell information. Det här knepet kan användas för uppgiftsstöld eller cyberspionage och kallas **social ingenjörskonst**. Det finns olika sätt att uppnå detta, men en vanlig metod är **nätfiske**, där e-postmeddelanden som verkar komma från tillförlitliga källor lurar användare att röja information eller klicka på länkar som infekterar enheter med nedladdade sabotageprogram. Mer än hälften av medlemsstaterna rapporterade om utredningar av nätverksangrepp[7].

Den kanske illvilligaste hottypen är **avancerade ihållande hot** (advanced persistent threat, APT). Det rör sig här om sofistikerade angripare som deltar i långsiktig övervakning och stöld av uppgifter, och ibland också har destruktiva mål. Syftet här är att hålla sig under radarn och undgå upptäckt så länge som möjligt. APT:er är ofta kopplade till stater och inriktade mot särskilt känsliga sektorer som teknik, försvar och kritisk infrastruktur. Cyberspionage påstås utgöra minst en fjärdedel av alla cyberincidenter och orsaka den största delen av kostnaderna[8].

Hur allvarligt är problemet?

07 På grund av att det saknas tillförlitliga data är det svårt att beskriva effekterna av att vara dåligt förberedd på ett cyberangrepp. Den ekonomiska effekten av it-brottslighet ökade femfaldigt mellan 2013 och 2017[9] och drabbade regeringar och såväl stora som små företag. Den prognostiserade ökningen av

cyberförsäkringspremier från 3 miljarder euro 2018 till 8,9 miljarder euro 2020 återspeglar den här trenden.

08 Samtidigt som cyberangreppens ekonomiska effekter fortsätter att öka finns det en alarmerande skillnad mellan kostnaden för att initiera ett angrepp och kostnaden för förebyggande, undersökning och reparation. Till exempel kan en DDoS-attack kosta så lite som 15 euro i månaden att utföra, men förlusterna för de drabbade företagen, inbegripet skadat anseende, är avsevärt högre[10].

09 Även om 80 % av företagen i EU upplevde åtminstone en cybersäkerhetsincident 2016[11] så är det fortfarande oroväckande få som medger riskerna. Bland företagen i EU har 69 % ingen, eller bara grundläggande, förståelse för sin exponering för cyberhot[12], och 60 % har aldrig uppskattat de eventuella ekonomiska förlusterna[13]. Enligt en global undersökning skulle dessutom en tredjedel av organisationerna hellre betala en hackares lösesumma än investera i informationssäkerhet[14].

10 Den globala utpressningstrojanen *Wannacry* och angreppen med det minerade sabotageprogrammet *NotPetya* 2017 påverkade sammanlagt fler än 320 000 offer i omkring 150 länder[15]. Dessa incidenter ledde till något av ett globalt uppvaknande kring hotet från cyberangrepp och gav ny fart åt insatserna för att få in cybersäkerhet i det allmänna politiska tänkandet. Dessutom tror 86 % av EU-medborgarna nu att risken för att falla offer för it-brottslighet ökar[16].

EU:s cybersäkerhetsåtgärder

11 EU blev en observatörsorganisation till Europarådets kommitté för konventionen om it-brottslighet år 2001[17] (Budapestkonventionen). Sedan dess har EU tillämpat politiska åtgärder, lagstiftning och finansiering för att förbättra sin cyberresiliens. Mot bakgrund av ett ökande antal stora cyberangrepp och -incidenter har verksamheten intensifierats sedan 2013, såsom visas i ***figur 2***. Parallellt därmed har medlemsstaterna antagit (och i vissa fall redan uppdaterat) sina första nationella strategier för cybersäkerhet.

12 De viktigaste EU-aktörerna med ansvar för cybersäkerhet beskrivs i ***ruta 2*** och ***bilaga I.***

Ruta 2

Vem deltar i arbetet?

Europeiska kommissionen strävar efter att stärka resurser och samverkan kring cybersäkerheten, stärka EU som en cybersäkerhetsspelare och integrera detta i övrig EU-politik. De generaldirektorat som främst har ansvar för cybersäkerhetspolitiken är **GD Kommunikationsnät, innehåll och teknik** (cybersäkerhet) och **GD Migration och inrikes frågor** (it-brottslighet), som ansvarar för den digitala inre marknaden respektive säkerhetsunionen. **GD Informationsteknik** ansvarar för it-säkerheten i kommissionens egna system.

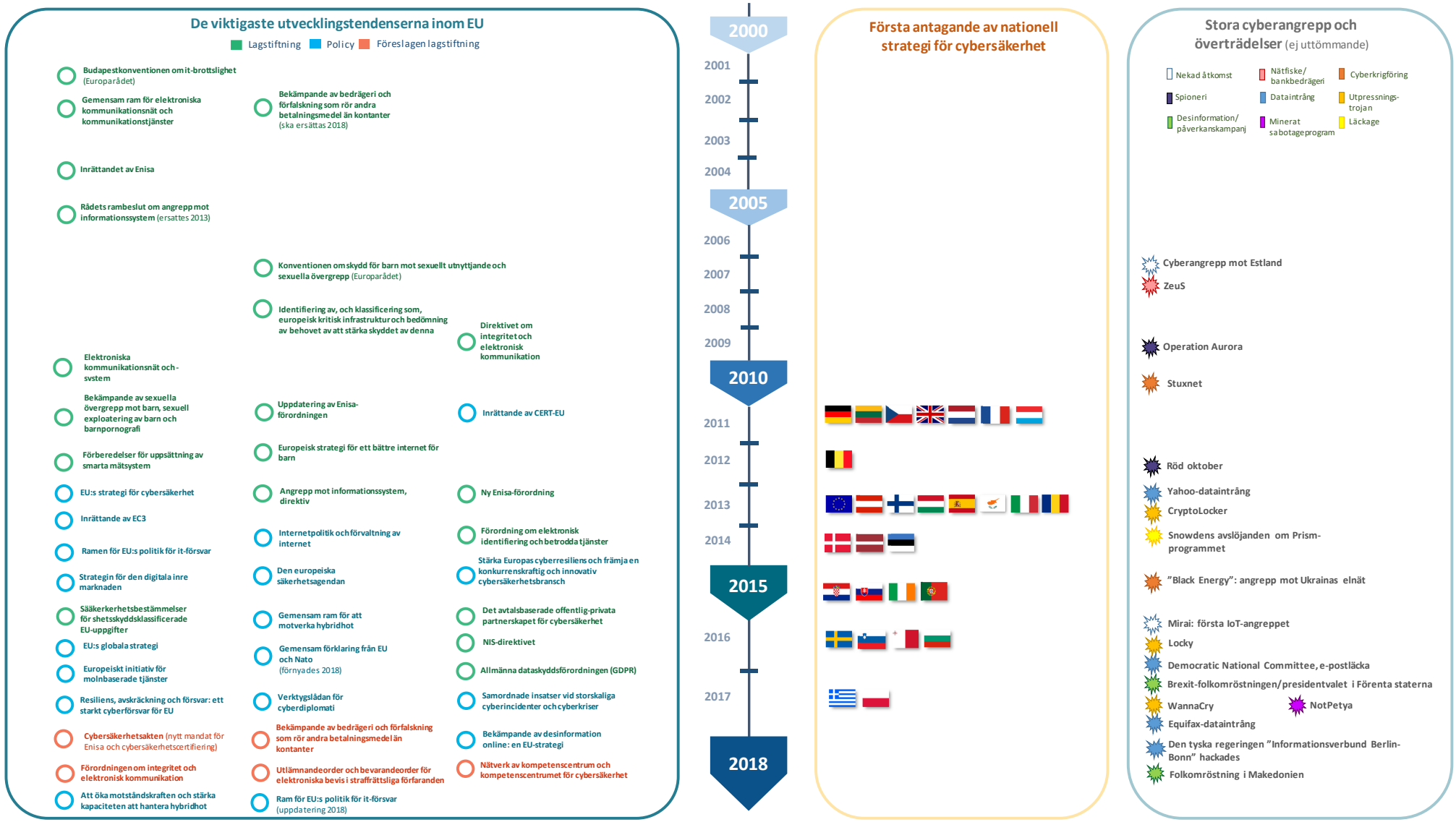
Ett antal EU-byråer stöder kommissionen, särskilt **Enisa** (Europeiska byrån för nät- och informationssäkerhet) som är EU:s cybersäkerhetsbyrå – ett först och främst rådgivande organ som stöder utveckling av politik, kapacitetsuppbyggnad och arbete för att öka medvetenheten. Europols europeiska it-brottscentrum (**EC3**) inrättades för att stärka EU:s brottsbekämpande insatser mot it-brottslighet. En incidenthanteringsorganisation (**CERT-EU**) som stöder alla unionens institutioner, organ och byråer drivs av kommissionen.

Europeiska utrikestjänsten har en ledande roll inom it-försvar, cyberdiplomati och strategisk kommunikation samt driver underrättelse- och analyscentrum. **Europeiska försvarsbyrån** (EDA) strävar efter att utveckla it-försvarskapaciteten.

Medlemsstaterna ansvarar först och främst för den egna cybersäkerheten och agerar på EU-nivå genom **rådet**, som har ett antal samordnande och informationsdelande organ (bland annat den övergripande arbetsgruppen för cyberfrågor). **Europaparlamentet** fungerar som medlagstiftare.

Organisationer i den privata sektorn, inbegripet industrin, internetförvaltningsorgan och den akademiska världen, är både partner och bidragsgivare till politisk utveckling och genomförande – inbegripet genom ett avtalsbaserat offentlig-privat partnerskap.

Figur 2 – Allt snabbare takt i utvecklingen av politik och lagstiftning (den 31 december 2018)



Källa: Revisionsrätten.

Politik

13 EU:s cyberekosystem är komplext och mångfacetterat och omfattar ett stort antal inrikespolitiska områden såsom rättsliga och inrikes frågor, den digitala inre marknaden och forskningspolitik. Inom utrikespolitiken är cybersäkerhet viktigt för diplomatin och spelar en allt viktigare roll i EU:s framväxande försvarspolitik.

14 Hörnstenen i EU:s politik är **strategin för cybersäkerhet från 2013**[18]. Strategin syftar till att göra EU:s digitala miljö säkrast i världen, samtidigt som grundläggande värden och friheter försvaras. Den har fem huvudsakliga mål: i) öka cyberresiliensen, ii) minska it-brottsligheten, iii) utveckla it-försvarspolitiken och -kapaciteten, iv) utveckla industriella och tekniska cybersäkerhetsresurser och, v) upprätta en internationell cyberrymdspolitik i linje med EU:s grundläggande värden.

15 Strategin för cybersäkerhet är sammanlänkad med tre strategier som antagits senare:

— Målet med den **europeiska säkerhetsagendan** (2015) är att förbättra brottsbekämpning och rättsliga åtgärder mot it-brottslighet, främst genom att förnya och uppdatera befintlig politik och lagstiftning[19]. Den syftar också till att identifiera hinder för rättsliga utredningar av it-brottslighet och förbättra cyberkapacitetsuppbyggnaden.

— Syftet med **strategin för den digitala inre marknaden**[20] (2015) är att förbättra tillgången till digitala varor och tjänster genom att skapa rätt villkor för att maximera den digitala ekonomins tillväxtpotential. I detta hänseende är det avgörande att stärka säkerhet, tillit och delaktighet online.

— Den **globala strategin**[21] från 2016 syftar till att främja EU:s roll i världen. Cybersäkerhet utgör en grundläggande pelare genom ett förnyat åtagande avseende cyberfrågor, samarbete med viktiga partner och ett beslut att hantera cyberfrågor inom alla politiska områden, inbegripet att motverka desinformation genom strategisk kommunikation.

16 Under senare år, i takt med att cyberrymden har blivit alltmer militariserad[22] och börjat användas som vapen[23] har den kommit att ses som det femte krigföringsområdet[24]. It-försvar skyddar cyberrymdens system, nätverk och kritiska infrastruktur mot angrepp med militära metoder eller andra slags metoder. En **ram för EU:s politik för it-försvar** antogs 2014 och uppdaterades 2018[25]. I uppdateringarna år 2018 identifieras sex prioriteringar, inbegripet utveckling av it-försvarskapacitet samt

skydd av kommunikations- och informationsnätverken för EU:s gemensamma säkerhets- och försvarspolitik (GSFP). It-försvar utgör också en del av det permanenta strukturerade samarbetet (Pesco) och EU-Nato-samarbetet.

17 EU:s **gemensamma ram för att motverka hybridhot** (2016) är inriktad på cyberhot mot både kritisk infrastruktur och privata användare och betonar att cyberangrepp kan genomföras genom desinformationskampanjer på sociala medier[26]. Inom ramen noteras också behovet av att förbättra medvetenheten och samarbetet mellan EU och Nato, vilket specificerades i de gemensamma förklaringarna från EU och Nato 2016 och 2018[27].

18 År 2017 presenterade kommissionen ett nytt cybersäkerhetspaket som återspeglade det växande behovet av digitalt skydd. Det inkluderade ett nytt meddelande från kommissionen om uppdatering av strategin för cybersäkerhet från 2013[28] och en plan för snabb och samordnad hantering av ett stort angrepp och för snabbt genomförande av direktivet om säkerhet i nätverks- och informationssystem (NIS-direktivet)[29]. Dessutom innehöll paketet ett antal lagstiftningsförslag (se punkt ***22***).

Lagstiftning

19 Sedan 2002 har lagstiftning med olika stor relevans för cybersäkerhet antagits.

20 Den viktigaste pelaren i strategin för cybersäkerhet från 2013 är **direktivet om nät- och informationssäkerhet (NIS)**[30] från 2016, den första EU-omfattande lagstiftningen om cybersäkerhet. Direktivet, som skulle införlivas senast i maj 2018, syftar till att uppnå en minsta nivå av harmoniserad kapacitet genom att ålägga medlemsstaterna att anta nationella NIS-strategier och skapa gemensamma kontaktpunkter och it-incidentcentrum (CSIRT-enheter)[31]. Det fastställer också säkerhets- och rapporteringskrav för leverantörer av samhällsviktiga tjänster i kritiska sektorer och för leverantörer av digitala tjänster.

21 Samtidigt trädde **den allmänna dataskyddsförordningen**[32] (GDPR) i kraft 2016 och började tillämpas i maj 2018. Syftet med den är att skydda de europeiska medborgarnas personuppgifter genom att upprätta regler för behandling och spridning av dessa. Den ger registrerade vissa rättigheter och ålägger personuppgiftsansvariga (leverantörer av digitala tjänster) skyldigheter avseende användning och överföring av information. Den inför också anmälningskrav vid överträdelser och i vissa fall kan böter

utfärdas. ***Figur 3*** visar hur NIS-direktivet och GDPR kompletterar varandra i sina syften att stärka cybersäkerheten och garantera dataskydd.

22 Bland de förslag till lagstiftning som för närvarande diskuteras finns den föreslagna cybersäkerhetsakten om att stärka Enisa och upprätta en EU-omfattande certifieringsmekanism[33], den föreslagna förordningen om utlämnandeorder och bevarandeorder för elektroniska bevis[34] och det föreslagna direktivet om elektroniska bevis[35]. Förslaget från 2018 om Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och nätverket av nationella samordningscentrum (nedan kallat *nätverk av kompetenscentrum för cybersäkerhet och ett kompetenscentrum för forskning*) utgör en del av cybersäkerhetspaketet från 2017[36].

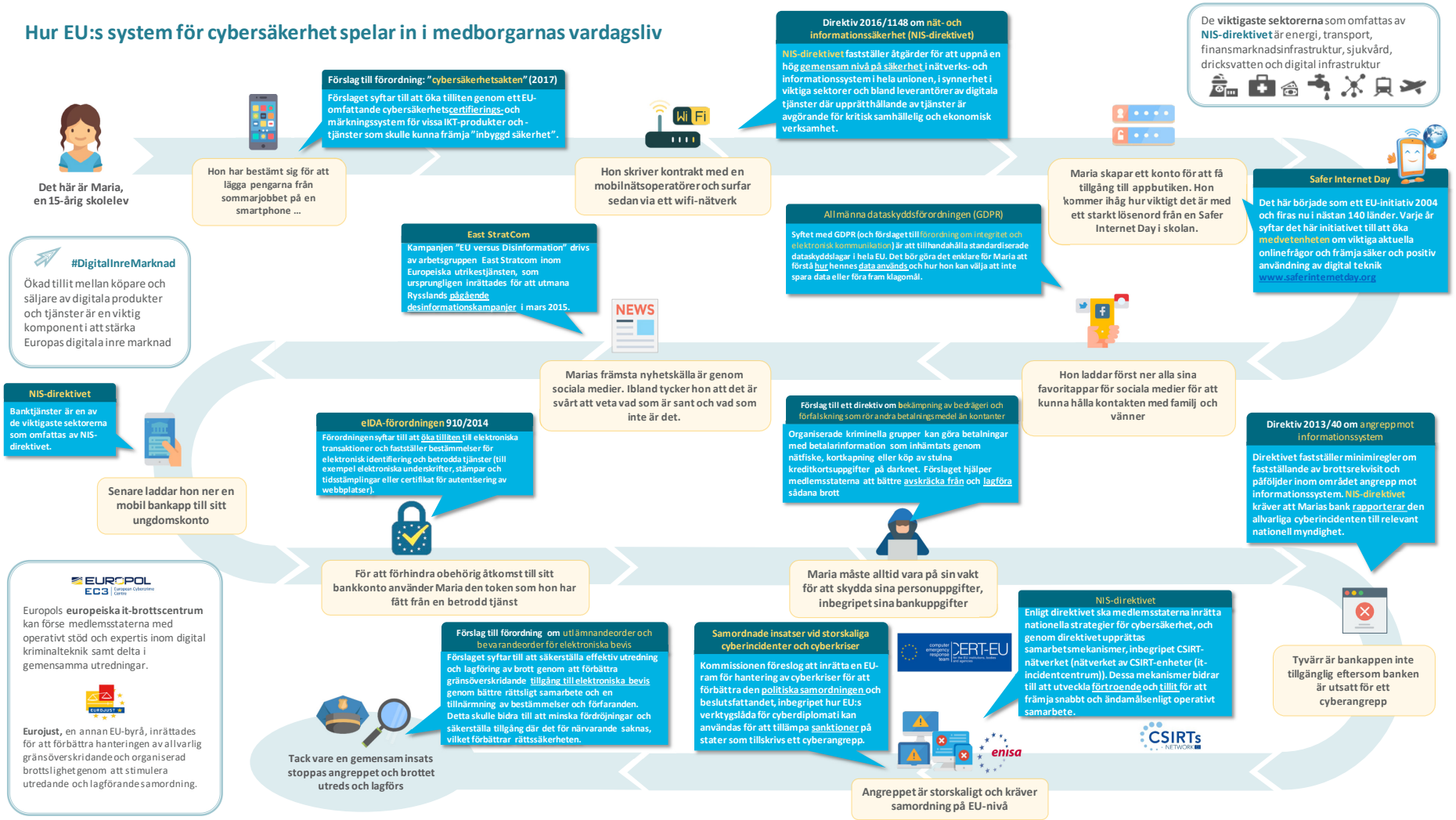
23 Det kan vara svårt att få en förståelse för den politiska och den rättsliga ramens bredd när det gäller cybersäkerhet och hur våra liv påverkas.

24 I ***figur 4*** görs ett försök att kartlägga hur olika lagstiftningsakter och annan verksamhet korsar en fiktiv europeisk medborgares liv.

Figur 3 – Hur GDPR och NIS-direktivet kompletterar varandra

Källa: Revisionsrätten.

Figur 4 – Hur EU:s system för cybersäkerhet spelar in i medborgarnas vardagsliv



Källa: Revisionsrätten.

Skapa en politisk och rättslig ram

25 EU:s cyberekosystem är komplext och mångfacetterat och har många aktörer (se ***bilaga I***). Det är en stor utmaning att sammanföra alla de olika delarna. Sedan 2013 har det funnits en samordnad insats för att skapa konsekvens på EU:s cybersäkerhetsområde[37].

Utmaning 1: meningsfull utvärdering och meningsfullt ansvarstagande

26 Det anses vara svårt att upprätta ett orsakssamband mellan strategin från 2013 och eventuella förändringar, som kommissionen har noterat. Målen med strategin från 2013 formulerades mycket brett och uttryckte en vision snarare än ett mätbart mål[38]. Då mätbara mål saknas är det en utmaning att ta fram åtgärder i linje med dessa breda syften. Den uppdaterade ramen för EU:s politik för it-försvar (2018) syftar till att utveckla mål för den miniminivå för cybersäkerhet och förtroende som ska uppnås. Detta begränsas dock till it-försvar, och några mål som definierar den önskade resiliensnivån för EU som helhet har inte fastställts.

27 Resultaten mäts sällan och få politikområden har utvärderats[39]. Detta beror delvis på att många av åtgärderna – lagstiftande eller andra – nyligen har genomförts, vilket innebär att deras effekter inte kan utvärderas fullt ut. Utmaningen är att definiera meningsfulla utvärderingskriterier som kan hjälpa till att mäta påverkan. Dessutom har strikt utvärdering fortfarande inte blivit norm för cybersäkerhet i allmänhet. Därför krävs en övergång till en resultatkultur med inbyggda utvärderingsmetoder och standardiserad rapportering. Enisas nuvarande mandat omfattar inte utvärdering och övervakning av statusen för EU:s cybersäkerhet och beredskap.

28 Evidensbaserat politiskt beslutsfattande är beroende av tillgången till tillräckliga tillförlitliga data och tillförlitlig statistik för att hjälpa till att övervaka och analysera trender och behov. Frånvaron av ett obligatoriskt och gemensamt övervakningssystem innebär att tillförlitliga data saknas. Indikatorer är inte direkt tillgängliga och svåra att definiera[40]. Specifika mått har dock utvecklats på vissa områden, till exempel inom EU:s policycykel avseende organiserad och grov internationell brottslighet.

29 Få medlemsstater samlar regelbundet in officiella uppgifter om cyberrelaterade frågor, vilket gör det svårt att jämföra. Hittills har EU inte gett mycket information om

behovet av att konsolidera statistik på europeisk nivå[41]. Det finns också få oberoende EU-omfattande analyser tillgängliga som omfattar viktiga frågor såsom[42] cybersäkerhetens ekonomi, inbegripet beteendeaspekter (diskrepans i incitament, informationsasymmetrier), förståelse för påverkan från cyberhaverier och it-brottslighet, makrostatistik kring cybertrender och förväntade utmaningar och de bästa lösningarna för att hantera hot.

30 Mot bakgrund av frånvaron av specifika mål och bristen på tillförlitliga data och väldefinierade indikatorer har bedömningen av strategins resultat hittills varit till största del kvalitativ. I lägesrapporter beskrivs utförda aktiviteter eller uppnådda milstolpar, utan någon noggrann mätning av resultaten. Dessutom har utgångsvärden för bedömningen av systemens resiliens ännu inte fastställts. På grund av att det inte finns någon kodifierad definition av it-brottslighet är det dessutom nästan omöjligt att hitta relevanta europeiska indikatorer som skulle vara till hjälp för övervakning och utvärdering.

31 Den oberoende översynen av genomförandet av cybersäkerhetspolitiken skiljer sig åt mellan medlemsstaterna. Vi genomförde en enkätundersökning bland de nationella revisionsorganen avseende deras erfarenhet av revisioner på detta område. Hälften av alla svarande[43] hade aldrig genomfört revisioner på området. Där revisioner hade genomförts låg fokus i huvudsak på informationshantering, skydd av viktig infrastruktur, informationsutbyte och samordning mellan berörda aktörer samt incidentberedskap, -rapportering och -hantering. Bland de ämnen som togs upp mer sällan fanns medvetandehöjande åtgärder och det digitala kompetensunderskottet. Resultaten av dessa revisioner eller utvärderingar offentliggörs inte alltid med hänsyn till den nationella säkerheten. En lista över offentliggjorda revisionsrapporter från de nationella revisionsorganen finns i ***bilaga III***.

32 Begränsad cyberrelaterad kompetens (se även punkterna ***82–90***) och svårigheter med att utvärdera framsteg i cybersäkerhet sågs som de största utmaningarna när det gäller att granska regeringars åtgärder på detta område.

Utmaning 2: hantera brister i EU-lagstiftningen och skillnader i införlivandet

33 Ny teknik och nya hot uppstår mycket snabbare än EU:s lagstiftning utformas och genomförs. Unionens förfaranden utformades inte med den digitala tidsåldern i åtanke: att utveckla innovativa och flexibla förfaranden för att säkerställa en politisk

och rättslig ram som är ändamålsenlig[44] för att bättre förutsäga och forma framtiden är en avgörande prioritering[45].

34 Trots att större enhetlighet eftersträvas är den rättsliga ramen för cybersäkerhet fortfarande ofullständig (några exempel finns i ***tabell 1***). Fragmentering och brister hämmar möjligheten att uppnå de övergripande politiska målen och leder till ineffektivitet. Bland de brister som kommissionen identifierat i sin strategiska bedömning finns sakernas internet, balansen av ansvar mellan användare och leverantörer av digitala produkter och vissa aspekter som inte tas upp i NIS-direktivet. I den föreslagna cybersäkerhetsakten görs delvis ett försök att ta itu med detta genom att främja inbyggd säkerhet genom ett EU-omfattande certifieringssystem. Vissa aktörer anser att en tydligt definierad cyberindustripolitik och ett gemensamt tillvägagångssätt för cyberspionage fortfarande är något som märkbart saknas[46].

Tabell 1 – Brister i den rättsliga ramen och skillnader i införlivandet (icke uttömmande)

Politikområde	Exempel
Digital inre marknad	o Det nuvarande direktivet om försäljning av konsumentvaror omfattar inte cybersäkerhet. De föreslagna direktiven om digitalt innehåll[47] och näthandel[48] syftar till att åtgärda dessa brister. o Det finns begränsade och olika rättsliga ramar för aktsamhetskrav i EU:s medlemsstater, vilket ger upphov till rättsosäkerhet och svårigheter att tillämpa rättsmedel[49]. o Riktlinjer för information om säkerhetsbrister i programvaror utvecklas med olika hastighet i medlemsstaterna och det finns inte någon övergripande rättslig ram på EU-nivå som möjliggör ett samordnat tillvägagångssätt[50].
Stärka nätverks- och informationssäkerhet	o Det står medlemsstaterna fritt att inkludera sektorer som utelämnas i NIS-direktivet[51]. Inkvarteringsbranschen, som inte omfattas, kan vara en inkörsport för andra brott, inbegripet människo- och droghandel och olaglig invandring[52].
Bekämpa it-brottslighet	o Många medlemsstater har inte definierat elektronisk bevisning i sin nationella lagstiftning[53] (se även punkt *22*). o Det aktuella rambeslutet om kontantlösa betalningsbedrägerier inbegriper inte uttryckligen icke-fysiska betalningsinstrument såsom virtuella valutor, elektroniska pengar och mobila pengar och det omfattar inte handlingar såsom nätfiske, kortkapning samt innehav och spridning av betalarinformation[54]. o Direktivet om angrepp mot informationssystem inriktar sig inte direkt på olaglig datainhämtning från insidan (t.ex. cyberspionage), vilket leder till utmaningar för brottsbekämpningen[55]. o Till följd av EU-domstolens dom om lagring av data[56] har skillnader i tillämpningen av den rättsliga ramen mellan medlemsstaterna hindrat brottsbekämpningen, vilket eventuellt har lett till förlust av ledtrådar i undersökningar och försämrat ändamålsenlig lagföring av kriminell verksamhet på nätet[57].

Källa: Revisionsrätten.

35 Tillämpning av vissa aspekter av lagstiftningen är frivillig för både nationella myndigheter och privata operatörer. Inom ramen för samarbetsgruppen är till exempel utvärdering av de nationella strategierna för säkerhet i nätverks- och informationssystem och CSIRT-enheternas ändamålsenlighet frivillig. Inom ramen för det föreslagna certifieringssystemet i cybersäkerhetsakten kommer också tillämpningen av certifiering för IKT-produkter och -tjänster att vara frivillig.

36 Inom EU är medlemsstaterna behöriga inom cybersäkerhet. Trots det spelar EU en avgörande roll i att skapa villkor för medlemsstaternas förmåga till förbättring och för att skapa samarbete och tillit mellan dem. Men oavsett de stora skillnaderna mellan medlemsstaterna när det gäller kapacitet och engagemang[58] är det fortfarande frivilligt att tillhandahålla känslig information (som rör nationell säkerhet).

37 Inkonsekvent införlivande av EU-lagstiftning bland medlemsstaterna kan leda till rättslig och operativ inkonsekvens och förhindra att lagstiftningen uppnår sin fulla potential. Till exempel har medlemsstaterna olika tolkningar av hur exportkontroller av produkter med dubbla användningsområden bör tillämpas[59], vilket medför att vissa EU-baserade företag eventuellt exporterar teknik och tjänster som kan användas för it-övervakning och människorättskränkningar genom censur eller avlyssning. Europaparlamentet har uttryckt oro angående detta[60].

38 För att skydda integriteten och yttrandefriheten krävs dessutom ett skräddarsytt lagstiftningsansvar i syfte att uppnå nödvändig balans mellan att skydda grundläggande värden och uppnå EU:s säkerhetsmål. Hur säkerställer vi till exempel totalsträckskryptering samtidigt som vi hittar det bästa sättet att stödja brottsbekämpningen? Och hur uppfyller vi målen med GDPR samtidigt som vi förstår hur förordningen påverkar offentligt tillgänglig information om registranter för domännamn och innehavare av IP-adressblock? Och vilka negativa effekter kan detta ha på brottsbekämpande utredningar[61]?

39 Enbart lagstiftning garanterar inte resiliens. Samtidigt som NIS-direktivets mål är att uppnå en hög säkerhetsnivå i hela EU är fokus uttryckligen inte att uppnå största möjliga harmonisering, utan en minimiharmonisering[62]. Brister kommer att fortsätta att uppstå i takt med att cyberlandskapet utvecklas.

Reflektionspunkter – politisk ram

- Vilka kritiska åtgärder krävs för att beslutsfattare och lagstiftare ska sträva mot en starkare resultatkultur inom cybersäkerhet, inbegripet en definition av övergripande resiliens?
- Hur kan forskning på ett bättre sätt bidra till att generera nödvändiga data och nödvändig statistik för att möjliggöra meningsfull utvärdering?
- På vilka sätt kan EU:s lagstiftningsprocesser anpassas så att de blir flexiblare och tar större hänsyn till hur snabbt tekniken och hoten utvecklas?
- Hur kan praxis för att utveckla mått (indikatorer, mål) i EU:s policycykel anpassas, skalas upp och överföras till cybersäkerhetsdomänen som helhet?
- Vad kan de nationella revisionsorganen lära sig från varandras tillvägagångssätt för revisioner av cybersäkerhetspolitik och -åtgärder?
- Vilka inkonsekvenser i införlivandet och genomförandet av EU:s rättsliga ram undergräver en mer ändamålsenlig hantering av brister när det gäller cybersäkerhet och it-brottslighet, och hur kan medlemsstaterna och EU-institutionerna hantera detta på bästa sätt?
- Hur ändamålsenliga är EU:s exportkontroller på cybervaror och -tjänster när det gäller att förebygga kränkningar av de mänskliga rättigheterna utanför EU?

Finansiering och utgifter

40 EU har siktet inställt på att ha världens säkraste onlinemiljö. För att nå det här målet krävs avsevärda insatser från alla aktörer, inbegripet en solid och väl förvaltad ekonomisk grund.

Utmaning 3: anpassa investeringsnivåerna till målen

Ökad investering

41 De totala globala utgifterna för cybersäkerhet uppskattas utgöra 0,1 % av BNP. I Förenta staterna[63] är denna siffra ungefär 0,35 % (inbegripet den privata sektorn). Förenta staternas federala regerings utgifter utgör kring 0,1 % av BNP eller cirka 21 miljarder dollar i budgeten för 2019[64].

42 I jämförelse har utgifterna i EU varit låga och fragmenterade, och ofta har de inte haft stöd av samordnade regeringsledda program. Det är svårt att hitta siffror, men EU:s offentliga utgifter för cybersäkerhet uppskattas ligga mellan en och två miljarder euro per år[65]. Vissa medlemsstaters utgifter i procent av BNP är en tiondel av motsvarande nivå i Förenta staterna, eller ännu lägre[66]. EU och medlemsstaterna måste veta hur mycket de sammanlagt investerar för att veta vilka brister som måste åtgärdas.

43 Det är svårt att få en heltäckande bild när det saknas tydliga data på grund av cybersäkerhetens övergripande karaktär och eftersom cybersäkerhet och allmänna it-utgifter ofta inte kan särskiljas[67]. Vår enkät har bekräftat att det är svårt att inhämta tillförlitlig statistik om utgifter i både offentlig och privat sektor. Tre fjärdedelar av de nationella revisionsorganen rapporterade att de inte har någon centraliserad översikt över cyberrelaterade offentliga utgifter, och inte i någon medlemsstat är det obligatoriskt för offentliga enheter att rapportera utgifter för cybersäkerhet separat i finansieringsplanerna.

44 Att öka offentlig och privat investering i Europas cybersäkerhetsföretag är en särskild utmaning. Offentligt kapital är ofta tillgängligt för de inledande faserna, men i mindre utsträckning för tillväxt- och expanderingsstadierna[68]. Det finns ett flertal EU-finansieringsinitiativ, men de utnyttjas inte, i stor utsträckning på grund av byråkrati[69]. I allmänhet underpresterar EU:s cybersäkerhetsföretag jämfört med sina internationella motsvarigheter: de är färre till antalet och den genomsnittliga

finansiering de får in är avsevärt lägre[70]. Det är därför avgörande att säkra ändamålsenlig målinriktning och finansiering av uppstartsföretag för att uppnå EU:s digitala politiska mål.

Ökad påverkan

45 Att åtgärda bristen på investeringar i cybersäkerhet måste leda till användbara resultat. Trots styrkan i EU:s forsknings- och innovationssektor är det inte alltid resultaten patenteras, kommersialiseras eller skalas upp i tillräcklig utsträckning för att stärka resiliensen, konkurrenskraften och den digitala autonomin[71]. Detta gäller särskilt i jämförelse med EU:s globala konkurrenter. Bristen på väl utnyttjade resultat beror på ett antal faktorer[72], inbegripet följande:

- Avsaknaden av en konsekvent transnationell strategi för att på ett bättre sätt möta EU:s bredare digitala behov och uppnå konkurrenskraft och ökad autonomi.
- Längden på värdekedjans cykel, vilken innebär att verktyg snart blir förlegade.
- Bristen på hållbarhet eftersom projekt vanligen avslutas med att projektgruppen blir upplöst, och support inbegripet uppdateringar och programfixar upphör.

46 Kommissionens förslag om att upprätta ett nätverk av kompetenscentrum för cybersäkerhet och ett kompetenscentrum för forskning är ett försök att överbrygga fragmenteringen på forskningsområdet för cybersäkerhet och sporra investeringar i stor skala[73]. Sammanlagt finns det ungefär 665 expertcentrum i hela EU.

Utmaning 4: en tydlig översikt över EU:s budgetutgifter

47 För transparens och förbättrad samordning är det viktigt med en centraliserad översikt över utgifterna. Om en sådan saknas är det svårt för beslutsfattarna att se hur utgifterna sammanfaller med behoven för att uppnå prioriterade mål.

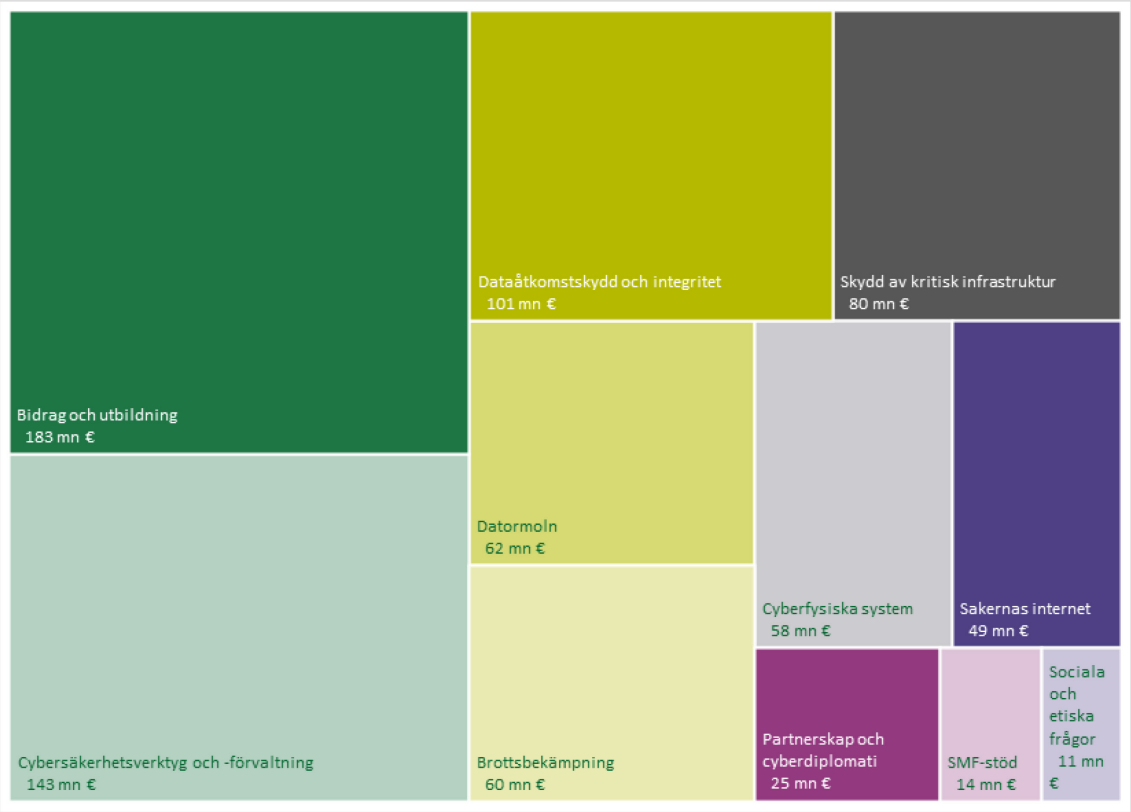
48 Det finns inte någon särskild budget som finansierar strategin för cybersäkerhet. På EU-nivå kommer cybersäkerhetsutgifterna i stället från EU:s allmänna budget och medlemsstaternas samfinansiering. Vår analys visar på en komplex struktur med minst tio olika instrument inom ramen för EU:s allmänna budget, men ingen tydlig bild av vilka pengar som går vart (se ***bilaga II***).

49 Det är alltså en riktigt stor utmaning att få en tydlig översikt över utgifterna för något som sträcker sig över många politiska områden. Utgiftsprogram förvaltas av olika avdelningar hos kommissionen, som alla har egna mål, regler och tidsplaner. Bilden kompliceras ytterligare om hänsyn tas till medlemsstaternas samfinansiering, såsom inom ramen för fonden för inre säkerhet (polisdelen)[74].

Identifierbara utgifter för cybersäkerhet

50 Under perioden 2014–2018 lade kommissionen minst 1,4 miljarder euro på att genomföra strategin för cybersäkerhet[75] varav den största delen gick via programmet Horisont 2020[76] (”H2020”). H2020-finansieringen fördelas främst genom programmet för säkra samhällen och genom projekt för ledarskap inom möjliggörande teknik och industriteknik[77]. Vi identifierade 279 kontrakterade cybersäkerhetsrelaterade projekt fram till september 2018, med en total EU-finansiering på 786 miljoner euro[78]. ***Figur 5*** visar dessa projekts typologi baserat på vår analys.

Figur 5 – H2020-kontrakterade forskningsprojekt för cybersäkerhet (miljoner euro)



Källa: Revisionsrätten.

51 Ett avtalsbaserat offentlig-privat partnerskap upprättades 2016 för att sporra EU:s cybersäkerhetsbransch. Syftet var att fördela 450 miljoner euro från H2020-programmet till det avtalsbaserade offentlig-privata partnerskapet och attrahera ytterligare 1,8 miljarder euro från den privata sektorn senast 2020. Under den 18 månader långa perioden fram till den 31 december 2017 fördelades 67,5 miljoner euro från H2020 till det avtalsbaserade offentlig-privata partnerskapet, och den privata sektorn investerade en miljard euro[79].

52 Kampen mot it-brottslighet stöds också av fonden för inre säkerhet – polisdelen (ISF-P). ISF-P stöder studier, expertmöten och kommunikationsinsatser som mellan 2014 och 2017 uppgick till nästan 62 miljoner euro. Medlemsstaterna kan dessutom få bidrag för utrustning, utbildning, forskning och datainsamling inom ramen för delad förvaltning. Nitton medlemsstater har fått bidrag på 42 miljoner euro.

53 Medel till stöd för rättsligt samarbete och genomförande av avtal om ömsesidig rättslig hjälp, med särskilt fokus på utbyte av elektroniska data och ekonomisk information, uppgick till nio miljoner euro inom ramen för programmet för rättsliga frågor som förvaltas av GD Rättsliga frågor och konsumentfrågor.

54 I NIS-direktivet anges uttryckligen att CSIRT-enheterna måste ha de resurser som de behöver för att effektivt utföra sina uppgifter[80]. Mellan 2016 och 2018 fanns 13 miljoner euro tillgängliga årligen från Fonden för ett sammankopplat Europa, som medlemsstaterna kunde ansöka om för att få hjälp med att genomföra kraven i direktivet. Ingen studie har gjorts för att fastställa de faktiska ekonomiska behoven för att CSIRT-nätverket och samarbetsgruppen ska nå effekt.

55 Flera av byråernas driftskostnader har varit särskilt avsedda för cybersäkerhet eller it-brott. Det är dock svårt att få fram exakta siffror från den offentligt tillgängliga informationen.

56 Budapestkonventionen (se punkt ***11***) har utgjort grunden för EU:s externa cyberutgifter. EU spenderade cirka 50 miljoner euro på att stärka cybersäkerheten bortom dess gränser under perioden 2014–2018. Nästan hälften av detta skedde genom instrumentet som bidrar till stabilitet och fred, med ett huvudsakligt projekt – GLACY+ med ett värde på 13,5 miljoner euro – som syftar till att världen över stärka kapaciteten att utveckla och genomföra lagstiftning om it-brottslighet och till att öka det internationella samarbetet[81]. Utgifterna inom ramen för EU:s andra finansieringsinstrument fokuserade i stor utsträckning på västra Balkan[82] samt det

europeiska grannskapet, till exempel Cybercrime@EaP-projektet med de östliga partnerskapsländerna som syftar till att förbättra internationellt samarbete inom it-brottslighet och elektroniska bevis.

Andra utgifter för cybersäkerhet

57 Det går inte alltid att identifiera specifika utgifter för cybersäkerhet inom ramen för EU-program:

- H2020-finansiering har också fördelats genom det gemensamma företaget Ecsel (Elektroniska komponenter och system för europeiskt ledarskap) för cyberfysiska system. Dock kunde vi inte fastställa vad som specifikt hade någon koppling till cybersäkerhet bland de 27 projekten mellan 2015 och 2016 som totalt uppgick till 437 miljoner euro.

- Upp till 400 miljoner euro finns tillgängliga för utgifter för cybersäkerhet och betrodda tjänster inom ramen för Europeiska struktur- och investeringsfonderna. Detta omfattar investeringar i säkerhet och dataskydd för att förbättra interoperabilitet och sammanlänkning av digital infrastruktur, elektronisk identifiering samt sekretess och betrodda tjänster.

58 I verksamhetsplanen för 2018 kungjorde Europeiska investeringsbanken sin avsikt att öka finansieringen av teknik med dubbla användningsområden, cybersäkerhet och civil säkerhet till upp till sex miljarder euro under en treårsperiod[83].

Framtidsutsikter

59 Cybersäkerhetskomponenten på två miljarder euro i det föreslagna nya programmet för ett digitalt Europa[84] (DEP) för 2021–2027 är utformad för att stärka EU:s cybersäkerhetsbransch och övergripande samhällsskydd, inbegripet genom att bidra till genomförandet av NIS-direktivet. Det föreslagna nätverket av kompetenscentrum för cybersäkerhet och ett kompetenscentrum för forskning, som syftar till att bana vägen för ett mer strömlinjeformat tillvägagångssätt, förväntas utgöra den huvudsakliga genomförandemekanismen för EU:s utgifter inom ramen för DEP.

60 Försvarsutgifterna inom ramen för EU-budgeten har nyligen ökat genom det europeiska försvarsindustriella utvecklingsprogrammet, med 500 miljoner euro som ska fördelas 2019 och 2020[85]. Fokus kommer att ligga på att förbättra samordningen och effektiviteten i medlemsstaternas försvarsutgifter genom incitament för

gemensam utveckling. Det syftar till att generera en försvarskapacitetsinvestering på sammanlagt 13 miljarder euro efter 2020 genom Europeiska försvarsfonden, som till viss del omfattar it-försvar[86].

Utmaning 5: lämpliga resurser till EU:s byråer

61 De tre viktigaste organen som står i centrum för EU:s cybersäkerhetspolitik – Enisa, Europols EC3 och CERT-EU (se ***ruta 2***) står inför utmaningar när det gäller resurser i en tid av ökade säkerhetsdrivna politiska prioriteringar. Med nuvarande tilldelning av mänskliga och ekonomiska resurser är det en utmaning för EU-byråerna att uppfylla förväntningarna[87].

62 Byråerna har begärt ytterligare resurser för att möta det ökade behovet, vilket dock inte har hörsammats fullt ut och eventuellt gör att politiska mål inte kan uppfyllas (i tid). Några exempel:

- Begränsade resurser var en faktor som hindrade Enisa från att fullt ut uppnå sina mål under 2017[88]. Ytterligare resurser föreslogs i paketet för 2017 som en anpassning till Enisas nya mandat.

- Tillgången till analytiker och investeringarna i IKT-kapacitet hos Europols EC3 har inte hållit takten med efterfrågan[89]. Europols och kommissionens gemensamma arbetsgrupp mot it-brottslighet (J-CAT) stöds dessutom av utplacerade experter från medlemsstaterna och tredjeland för underrättelseledda utredningar. Dock bärs kostnaderna främst av de utskickande staterna, vilket motverkar utplacering av ett större antal experter. En tillfällig, fallbaserad lösning för utplacering har utformats med viss finansiering genom Europol eller EU:s policycykel för att möjliggöra för fler länder att delta.

63 Vissa begränsningar är självförvållade. Många anställda på CERT-EU och Enisa är kontraktsanställda och det tar ofta lång tid att rekrytera dem. Andra begränsningar, såsom svårigheten att attrahera och behålla talanger, beror på byråernas oförmåga att konkurrera med lönerna i den privata sektorn eller på dåliga möjligheter till karriärutveckling. Enisa lade därför ut mycket av sitt arbete på entreprenad mellan 2014 och 2016[90].

64 Brist på personal och nödvändiga verktyg kan medföra avsevärda risker, i synnerhet avseende inhämtning av underrättelser om hot. Datamängden från öppna och stängda källor fortsätter att öka och riskerar att överväldiga analytikernas förmåga

att utföra korrekta hotanalyser. Om rätt kapacitet och verktyg saknas för att integrera och sammanlänka data blir det svårt att få fram användbara underrättelser om hot som kan delas och analyseras i hela EU[91].

Reflektionspunkter – finansiering och utgifter

- På vilka sätt kan kommissionen och lagstiftarna strömlinjeforma EU:s utgifter för cybersäkerhet och mer uttryckligt anpassa dem till tydligt definierade mål?
- Hur kan bristerna i EU-byråernas resurser hanteras på ett övergripande sätt som tar hänsyn till unionens behov och mål?
- Vilka åtgärder identifieras på EU- och medlemsstatsnivå för att minska hindren för små- och medelstora företag som mottar investeringskapital för att bygga ut sin verksamhet?
- Vilka konkreta och oavbrutna resultat bidrar H2020-medlen med när det gäller cybersäkerhetslösningar?
- På vilket sätt stärker EU:s kapacitetsuppbyggande verksamhet kapacitet utanför unionens gränser i linje med EU:s värden?

Skapa ett samhälle präglat av cyberresiliens

65 Styrning av cybersäkerhet innefattar förvaltning av hot och risker, stärkande av kapacitet och medvetenhet samt samordning och informationsutbyte som bygger på grundläggande tillit.

Utmaning 6: stärka styrning och standarder

Styrning av informationssäkerhet

66 Styrning av informationssäkerhet handlar om att upprätta strukturer och politik för att säkerställa konfidentialitet, integritet och tillgänglighet för data. Det här är mer än en teknisk fråga; den kräver ändamålsenligt ledarskap, robusta processer och strategier som går i linje med organisatoriska mål[92]. Styrning av cybersäkerhet ingår som en del i styrningen av informationssäkerheten och omfattar alla slags cyberrelaterade hot, inbegripet målinriktade, sofistikerade angrepp, överträdelser eller incidenter som är svåra att upptäcka eller förvalta.

67 Modellerna för styrning av cybersäkerhet skiljer sig åt mellan medlemsstaterna och i medlemsstaterna är ansvaret för cybersäkerhet ofta uppdelat på många olika enheter. Dessa skillnader kan utgöra ett hinder för det samarbete som krävs för att hantera storskaliga, gränsöverskridande incidenter och för att utbyta underrättelser om hot, framför allt på EU-nivå men också nationellt. Vår enkät bland de nationella revisionsorganen visade att svagheter i de offentliga myndigheternas styrformer och riskhantering sågs som de största riskerna.

68 Trots att konsekvenserna för organisationer i den privata sektorn kan vara allvarliga finns det många svagheter i cyberstyrningen. Nästan nio av tio organisationer anger att deras cybersäkerhetsfunktion inte fullt ut motsvarar deras krav[93] och cybersäkerhetsansvariga befinner sig ofta minst två nivåer bort från styrelsen[94].

69 I EU:s bolagsrättsdirektiv finns det inte några särskilda krav på att informera om cyberrisker. I Förenta staterna utfärdade Securities and Exchange Commission nyligen icke-bindande riktlinjer till hjälp för offentligägda företag att utarbeta information om cybersäkerhetsrisker och -incidenter[95]. Den gemensamma kommittén för de

europeiska tillsynsmyndigheterna[96] varnade för de ökade cyberriskerna samt uppmanade finansinstitut att förbättra känsliga it-system och att utforska inneboende risker för informationssäkerhet, anslutningskapacitet och utlokalisering[97].

70 Det är särskilt svårt att stärka styrningen av informationssäkerhet på små och medelstora företag eftersom de ofta inte kan införa lämpliga system. Små och medelstora företag saknar relevanta riktlinjer för tillämpning av kraven på informationssäkerhet och integritet och begränsning av de tekniska riskerna[98]. De viktigaste utmaningarna är därför att bättre förstå deras behov och tillhandahålla nödvändiga incitament och nödvändigt stöd.

71 Avsaknaden av ett konsekvent, internationellt ramverk för styrning av cybersäkerhet påverkar det internationella samfundets förmåga att hantera och begränsa cyberangrepp. Det är därför viktigt att skapa samförstånd kring en sådan styrningsram som på bästa sätt återspeglar EU:s intressen och värden[99]. Försöken att upprätta bindande internationella cyberrymdsstandarder präglas alltmer av spänningar, vilket sågs i bristen på samförstånd i FN-gruppen med myndighetsexperter år 2017 om hur internationell lagstiftning bör tillämpas på staters hantering av incidenter.

72 För att stärka sin agenda när det gäller styrning av cyberrymden har EU också formaliserat sex cyberpartnerskap i syfte att upprätta regelbundna politiska dialoger som strävar efter att bygga tillit och gemensamma samarbetsområden[100]. Resultaten är blandade, men på det hela taget kan EU fortfarande inte ses som en stor aktör inom cybersäkerhet i det internationella samfundet, trots att dess profil har höjts[101].

Informationssäkerhet vid EU:s institutioner

73 Varje EU-institution har egna bestämmelser om styrning av informationssäkerhet. Ett interinstitutionellt avtal tillhandahåller assistans för informationssäkerhet från kommissionen till de andra institutionerna och byråerna. EU:s institutioner och organ har identifierat behovet av att utveckla sin cyberkapacitet och sina metoder för riskhantering på ett konsekvent sätt. Kommissionen, rådet och Europeiska utrikestjänsten ska 2020 presentera en rapport för den övergripande arbetsgruppen för cyberfrågor om styrning och de framsteg som gjorts när det gäller att klargöra och harmonisera styrningen av cybersäkerhet vid EU:s institutioner och byråer[102].

74 Inom kommissionen ansvarar generaldirektoratet för informationsteknik för it-infrastrukturens och tjänsternas säkerhet (se ***ruta 3***). De främsta it-säkerhetsmålen för kommissionens digitala strategi är att införliva it-säkerhet i styrningsprocesserna,

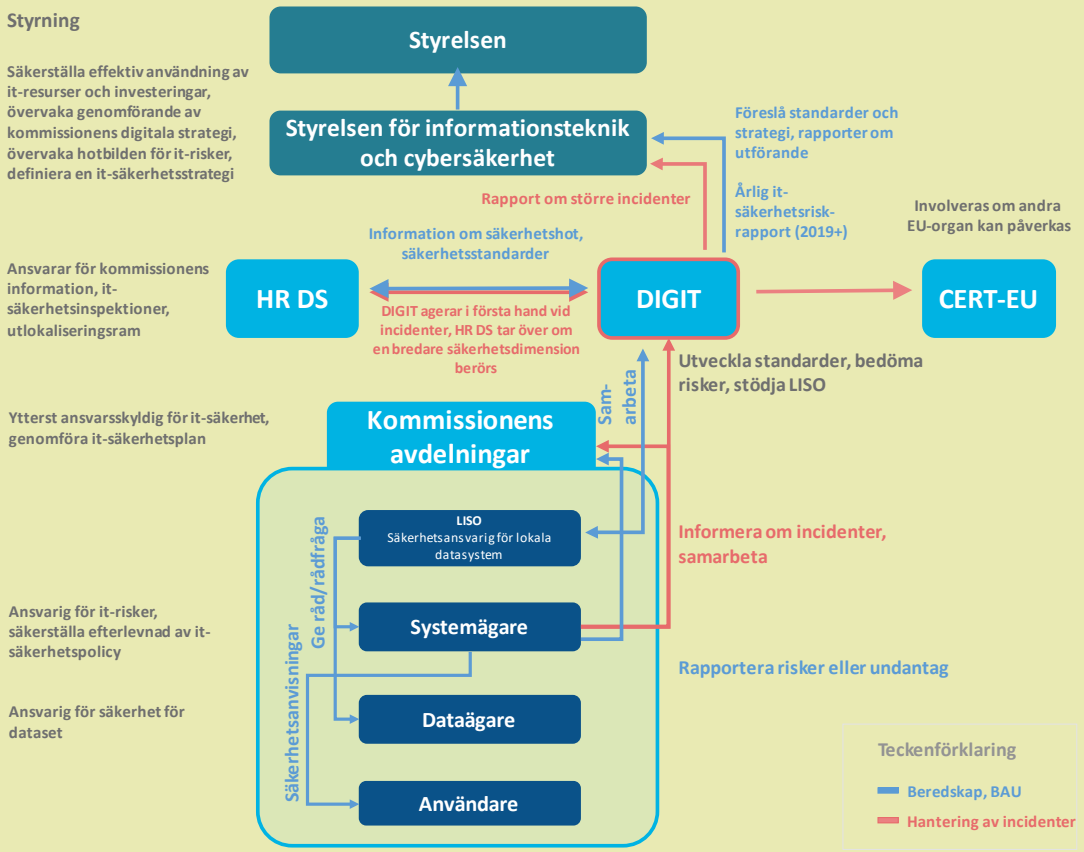
tillhandahålla (kostnadseffektiv och) ändamålsenlig infrastruktur och resiliens, utöka omfattningen av detektering och hantering av incidenter och integrera it- och säkerhetsstyrning[103]. Inom ramen för sitt leverantörsavtal säkerställer kommissionen att nästan all programvara aktivt underhålls och att endast leverantörsstödd programvara används[104].

75 Vikten av att skydda institutionerna sträcker sig också till EU:s GSFP-uppdrag och GSFP-strukturer världen över. En av prioriteringarna i EU:s ram för politiken för it-försvar (uppdateringen från 2018) är att förbättra skyddet av de GSFP-relaterade kommunikations- och informationssystem som EU-enheterna använder. En intern styrelse för cyberstyrning inom Europeiska utrikestjänsten har nu upprättats och sammanträdde för första gången i juni 2017[105].

Ruta 3

Skydda kommissionens informationssystem

Kommissionens omkring 1 300 system och 50 000 enheter utsätts hela tiden för cyberangrepp. Ansvaret för it är decentraliserat i enlighet med figuren nedan. Informations- och it-säkerhet utgår från en gemensam it-säkerhetsplan som GD Informationsteknik har upprättat. Styrelsen för informationsteknik och cybersäkerhet fungerar i praktiken som kommissionens informationssäkerhetschef och kopplar samman it-säkerhetens operativa sida med kommissionens högsta ledning som utgörs av styrelsen.



Källa: Revisionsrätten, på grundval av kommissionens beslut[106].

Generaldirektoratet för personal och säkerhet har som främsta uppgift att skydda kommissionens personal, information och tillgångar. Det utför också säkerhetsundersökningar av incidenter som har en bredare säkerhetsdimension än bara it, och använder resultaten för åtgärder som rör kontraspionage och terrorismbekämpning.

GD Informationsteknik ansvarar för it-säkerhet och driver CERT-EU (incidenthanteringsorganisationen). CERT-EU upprättades 2011 och drivs med en årlig budget på cirka 2,5 miljoner euro samt har ungefär 30 anställda. Organisationen är den som agerar i första hand vid informationssäkerhetsincidenter som berör flera

institutioner, men är inte verksam dygnet runt. Den driver en plattform för informationsutbyte. År 2018 undertecknade CERT-EU ett icke-bindande samförståndsavtal med Enisa, EC3 och Europeiska försvarsbyrån för att stärka samarbetet och samordningen. Den har också en teknisk överenskommelse med Natos it-incidenthanteringsorgan (NCIRC).

Hotbilder och riskbedömningar

76 Välgrundade och kontinuerliga hot- och riskbedömningar är viktiga verktyg för både offentliga och privata organisationer. Det finns dock inte något standardiserat tillvägagångssätt för att klassificera och kartlägga cyberhot eller utföra riskbedömningar, vilket innebär att innehållet i bedömningarna varierar avsevärt, något som utgör en utmaning för en konsekvent, EU-omfattande strategi för cybersäkerhet[107]. Dessutom förlitar sig hotbedömningarna ofta på samma källor, eller till och med andra hotbedömningar, vilket leder till att samma resultat hela tiden upprepas[108] samtidigt som risken är stor att andra hot inte uppmärksammas tillräckligt. Detta förvärras av en fortsatt ovilja att utbyta information och en underrapportering av incidenter.

77 EU:s gemensamma enhet för hybridhot[109], som är en del av Europeiska utrikestjänsten, inrättades för att förbättra situationsmedvetenheten och stödja beslutsfattandet genom utbyte av analyser, men måste bredda sin expertis, inbegripet inom cybersäkerhet. Samtidigt förser CERT-EU EU:s institutioner, organ och byråer med rapporter och genomgångar om cyberhot mot dem.

78 Enisa har tidigare noterat att många medlemsstater gör en kvalitativ bedömning av hot och att det finns ett behov av mer cyberhotsmodellering[110]. Övervakning av kapaciteten för strategisk analys kommer att leda till en bättre samlad bedömning. Dock skulle hotbedömningarna kunna omfatta inte bara tekniska hot, utan också sociopolitiska och ekonomiska hot för att säkerställa en mer heltäckande bild, samt drivkrafter bakom hot och aktörernas motiv.

Incitament

79 Det finns fortfarande för få rättsliga och ekonomiska incitament för organisationer att rapportera och dela information om incidenter. Många organisationer är rädda om sitt rykte och föredrar fortfarande att hantera cyberangrepp diskret eller betala förövarna. Det återstår att se hur ändamålsenligt NIS-direktivet blir när det gäller att öka rapporteringsnivån. Kommissionen förväntar

sig att förbättringar kommer att ske främst på nationell nivå, men cybersäkerhetsakten kommer att tillföra ett EU-omfattande perspektiv.[111]

80 Genom att tillämpa vissa standarder i sina upphandlingar har offentliga myndigheter stor möjlighet att påverka leverantörer som inköpare av digitala produkter och tjänster genom offentlig upphandling samt forsknings- och programfinansiering (till exempel genom att kräva att vissa tekniska standarder tillämpas, såsom internetprotokollet IPv6, för att bidra till kampen mot it-brottslighet). För närvarande finns det dock inte någon gemensam upphandlingsram för cybersäkerhetsinfrastruktur[112]. Här finns det mycket som kommissionen kan göra. Det föreslagna programmet för ett digitalt Europa för nästa fleråriga budgetram syftar till att hantera den offentliga sektorns hittills begränsade investeringar i inköp av den senaste cybersäkerhetstekniken.

81 Genom sin lagstiftningskapacitet kan kommissionen säkerställa att rätt standarder utvecklas för att lösningar som förbättrar säkerheten ska antas på bred front. Kommissionen och Europol arbetar tillsammans med internetförvaltningsorgan som ICANN (se punkt ***38***) och RIPE-NCC[113], vilket är avgörande för att få rätt arkitektur på plats till stöd för de rättsliga myndigheternas it-brottsbekämpning.

Utmaning 7: öka kompetensen och medvetenheten

82 Enisa har poängterat att användarna spelar en viktig roll i kampen mot cyberangrepp och att det är avgörande för ett samhälle präglat av cyberresiliens att stärka kompetens, utbildning och medvetenhet[114]. Människor som hemma eller på jobbet har god förmåga att upptäcka varningstecken och har utrustats med rätt teknik kan fördröja eller förhindra angrepp.

83 Ett stort bekymmer är det växande gapet mellan den kunskap som krävs för att begå ett it-brott eller inleda ett cyberangrepp och den kompetens som krävs för att avvärja dessa. Brott som nättjänst-modellen har gjort det enklare att ta sig in på it-brottsmarknaden: människor utan teknisk kunskap att bygga dem kan nu hyra botnät, ”exploit kits” eller utpressningstrojanpaket.

Utveckling av utbildning, kompetens och kapacitet

84 Världen över ökar bristen på kompetens inom cybersäkerhet. Arbetskraftsunderskottet har ökat med 20 % sedan 2015[115]. De traditionella rekryteringskanalerna uppfyller inte efterfrågan, inbegripet för ledande och

tvärdisciplinära befattningar[116]. Nästan 90 % av dem som arbetar med cybersäkerhet världen över är män, och den konstanta bristen på jämn könsfördelning begränsar talangpoolen ytterligare[117]. På universiteten är cyberrelaterade ämnen dessutom underrepresenterade på andra program än de tekniska.

85 Utbildning behövs på alla plan, bland statstjänstemän och tjänstemän inom brottsbekämpande myndigheter, rättsliga myndigheter och väpnade styrkor samt lärare. Till exempel måste domstolarna kunna hantera de snabbt föränderliga tekniska särdragen i it-brottslighet och offren för denna[118]. Just nu saknas EU-omfattande standarder för utbildning och certifiering[119]. Vid EU-institutionerna är det viktigt att ha rätt blandning av kompetens. Om den rätta kompetensmixen saknas kan institutionerna få svårt att på ett korrekt sätt definiera ramar, identifiera rätt partner, bedöma säkerhetsbehov eller i förlängningen förvalta program. Detta kan i sin tur undergräva EU-programmens eller den politiska utvecklingens ändamålsenlighet.

86 Visserligen ansvarar medlemsstaterna för utbildningspolitiken på EU-nivå, men ett flertal utbildningsaktiviteter (se ***tabell 2***) och övningar (se ***ruta 4***) utförs redan. EU kan bidra med att införliva EU-omfattande standarder i läroplanerna i alla relevanta discipliner[120]. På exempelvis området digital kriminalteknik behövs gemensamma utbildningsstandarder för att underlätta vägen mot ömsesidig tillåtlighet av bevis mellan medlemsstaterna. På grund av it-brottslighetens gränsöverskridande natur kan ett flertal jurisdiktioner vara involverade, vilket kräver utbildning på EU-nivå. Trots det har Cepol, EU:s byrå för utbildning inom brottsbekämpning, noterat att mer än två tredjedelar av medlemsstaterna inte tillhandahåller regelbunden utbildning till brottsbekämpande tjänstemän[121]. Eventuellt kan EU också identifiera sätt att skapa synergieffekter mellan utbildning på det civila och det militära området[122]. Med det sagt har Enisa funnit att trots att de viktiga utbildningsmöjligheterna i kritiska sektorer är omfattande så omfattas resiliensen för kritisk infrastruktur inte i tillräcklig utsträckning[123].

Tabell 2 – Några av EU:s cyberrelaterade utbildningsinitiativ

Europeiska försvarsbyråns projekt, till exempel utbildningsstöd från den privata sektorn och projektet Cyber Ranges	Europeiska säkerhets- och försvarsakademins nätverk (som tillhandahåller civil-militär utbildning), inbegripet cyberutbildning, träningsövningar och utvärderingsplattformar	Enisa-utbildning, som erbjuder utbildningsprogram där den kommersiella marknaden eventuellt inte gör det
Europols, Cepols och ECTEG:s[124] utbildningsprogram – inbegripet modellen för utbildningsstyrning och ramen för utbildningskompetens (inkl. certifiering)	Nätverket av kompetenscentrum och kompetenscentrumet för forskning (förslag)	Krypteringsåtgärder föreslagna i den elfte rapporten om säkerhetsunionen
Samarbetet mellan EU och Nato om cyberförsvarsutbildning	Militära Erasmus-programmet	Det europeiska nätverket för rättslig utbildning

Källa: Revisionsrätten.

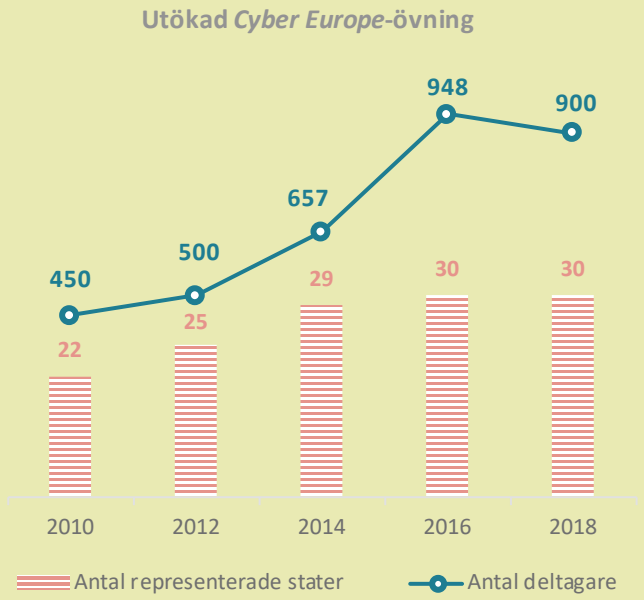
87 EU har stationerat experter på terrorismbekämpning och säkerhet i 17 delegationer för att stärka länken mellan EU:s interna och externa säkerhet[125]. Trots de begränsade resurserna kan ökad cyberkunskap bidra till att man satsar på rätt projekt och identifierar synergieffekter med andra program eller källor till finansiering[126]. Det kan också kunna höja cybersäkerhetens profil i den politiska dialogen, trots konkurrensen med många andra prioriteringar såsom migration, organiserad brottslighet eller återvändande utländska stridande.

Ruta 4

Övningar

Övningar är viktiga element i cyberutbildning som ger goda möjligheter att öka beredskapen genom att testa kompetenser, hantera verkliga scenarier och bygga nätverk av arbetsrelationer. Sedan 2010 har de ökat markant.

Deltagarna deltar på plats eller på distans. Efter övningarna genomförs utvärderingar för att identifiera lärdomarna, även om de fortfarande inte helt och hållet har trängt igenom de strategiska/politiska, operativa och tekniska lagren[127].



Källa: Revisionsrätten, baserat på dokument från Enisa.

EU:s och Natos flaggskeppsövningar – Cyber Europe vartannat år (operativt) och Locked Shields varje år (tekniskt) – samlar över 1 000 deltagare från cirka 30 deltagande stater. Båda övningarna fokuserar på att skydda och underhålla kritisk infrastruktur i simulerade angreppscenarier. Övningarnas räckvidd har ökat avsevärt och båda innefattar nu media samt rättsliga och ekonomisk-politiska element för att förbättra de yrkesverksammas situationsmedvetenhet. De parallella och samordnade (strategiska) PACE-övningarna testar EU:s och Natos samspel i ett hybridkrisscenario.

Det här är inte de enda internationella övningarna. Enisa organiserar en årlig cyberutmaning där lag tävlar i att lösa säkerhetsrelaterade utmaningar inom webb- och mobilsäkerhet, kryptogram, reverse engineering, etik och kriminalteknik. Den första övningen på ministernivå, EU Cybrid, genomfördes i september 2017 och fokuserade på strategiskt beslutsfattande. År 2018 inleddes samarbetsövningen med Nato, Crossed Swords, i syfte att förbättra de offensiva elementen i Locked Shields-övningen. Nato organiserar också Cyber Coalition-övningen.

En viktig utmaning är att säkerställa att alla viktiga aktörer är aktivt involverade och att alla övningar samordnas för att undvika dubbelarbete och dela lärdomar effektivt.

Medvetenhet

88 Angrepp och desinformation sprids ofta via medborgarna eftersom de många gånger oavsiktligen utsätts för säkerhetsbrister genom billiga och vitt spridda programvaror eller faller offer för social ingenjörskonst. Ökad medvetenhet är därför avgörande för att bygga upp ändamålsenlig cyberresiliens, men det är knappast en enkel uppgift eftersom det är svårt för lekmän att förstå cybersäkerhetens komplexitet och de tillhörande riskerna.

89 Den årliga europeiska månaden för it-säkerhet (ECSM) och Safer Internet Day är exempel på åtgärder för att öka medvetenheten. Sju länder som inte är med i EU har nu gått med i ECSM[128]. Europols *Say No!*-kampanj syftar till att minska risken för att barn faller offer för sexuellt tvång och sexuell utpressning online. Det är viktigt att minska risken eftersom få offer för angrepp för närvarande anmäler dessa brott till polisen[129]. Kommissionen erkänner att strategin för cybersäkerhet endast har varit delvis ändamålsenlig när det gäller att öka medvetenheten bland medborgarna och företagen[130]. Det här beror på uppgiftens storlek, begränsade resurser, medlemsstaternas olika engagemang och en brist på vetenskapliga bevis på hur man bäst ökar och mäter medvetenhet.

90 Utmaningen för kommissionen och de relevanta byråerna är att säkerställa att åtgärderna för att öka medvetenheten är målinriktade och förmedlas på ett bra sätt, att de är inkluderande, följer hotbilderna, undviker oavsiktliga effekter såsom ”säkerhetsutmattning”[131] och utvecklar utvärderingsmetoder och mått för att bedöma ändamålsenligheten. Detta bör också gälla på EU-institutionerna, där medvetenhetskulturen måste förbättras[132].

Utmaning 8: bättre utbyte och samordning av information

91 Cybersäkerhet kräver samarbete mellan offentlig och privat sektor, först och främst genom utbyte av information och bästa praxis. Tillit är avgörande på alla nivåer för att skapa rätt miljö för utbyte av känslig information över gränserna. Dålig samordning leder till fragmentering, dubbelarbete och utspridd expertis. Ändamålsenlig samordning kan leda till påtaglig framgång, såsom nedstängning av darkweb-marknadsplatser[133]. Trots de framsteg som har gjorts under de senaste åren är tillitsnivåerna fortfarande otillräckliga[134] på EU-nivå och i vissa medlemsstater[135].

Samordning mellan EU:s institutioner och medlemsstater

92 Ett av syftena med strategin för cybersäkerhet och de kooperativa strukturer som infördes genom NIS-direktivet har varit att stärka tilliten mellan aktörerna. I utvärderingen av strategin erkändes att en grund lagts för strategiskt och operativt samarbete på EU-nivå[136]. Trots det är samordningen i allmänhet otillräcklig[137]. Utmaningen är att säkerställa att utbyte av information inte bara är meningsfullt utan också ger en översikt över helheten. Att uppnå gemensam förståelse baserat på accepterad terminologi är en viktig faktor i detta hänseende (se ***ruta 5***).

93 I Enisas utvärdering noterades dock att EU:s strategi för cybersäkerhet inte samordnades i tillräcklig utsträckning, vilket ledde till bristande synergieffekter mellan Enisas verksamhet och andra aktörers. Samarbetsmekanismerna är fortfarande relativt outvecklade[138] och cybersäkerhetsakten syftar till att ta itu med detta genom att stärka Enisas samordnande roll. Önskan att förbättra samarbetet var den logiska grunden bakom samförståndsavtalet som tecknades 2018 mellan Enisa, EDA, Europols EC3 och CERT-EU[139]. Under de kommande åren kommer kommissionen att prioritera att säkerställa att politiska initiativ, behov och investeringsprogram går i linje med varandra i syfte att överbrygga fragmentering och skapa synergieffekter[140].

94 Samordningsfunktioner är införlivade i olika institutionella organ. Arbetsgruppen för säkerhetsunionen inrättades för att spela en central roll i samordningen av kommissionens olika generaldirektorat i syfte att stödja säkerhetsunionens agenda[141]. GD Kommunikationsnät, innehåll och teknik är ordförande i arbetsgruppens underarbetsgrupp om cybersäkerhet.

95 I rådet hanteras cybersäkerhet av den övergripande arbetsgruppen för cyberfrågor som samordnar strategiska och horisontella cyberfrågor och bidrar till att förbereda övningar och utvärdera resultaten av dem. Den har ett nära samarbete med kommittén för utrikes- och säkerhetspolitik, som har en central beslutsfattande roll avseende alla cyberrelaterade diplomatiska åtgärder (se ***ruta 6*** i nästa kapitel). Eftersom cybersäkerhet är ämnesövergripande är det inte enkelt att samordna alla relevanta intressen: inte mindre än 24 arbetsgrupper och förberedande organ har nyligen hanterat cyberrelaterade frågor[142].

96 De två senaste lagstiftningsförslagen om att stärka Enisa (2017) och inrätta ett nätverk av kompetenscentrum för cybersäkerhet och ett kompetenscentrum för forskning (2018) är särskilt utformade för att ta itu med fragmenteringen och dubbelarbetet. En drivande faktor bakom nätverket av kompetenscentrum för

cybersäkerhet och ett kompetenscentrum för forskning har varit att åtgärda de brister som NIS-direktivets kooperativa strukturer inte åtgärdar eftersom de inte utformades för att stödja utvecklingen av spetslösningar.

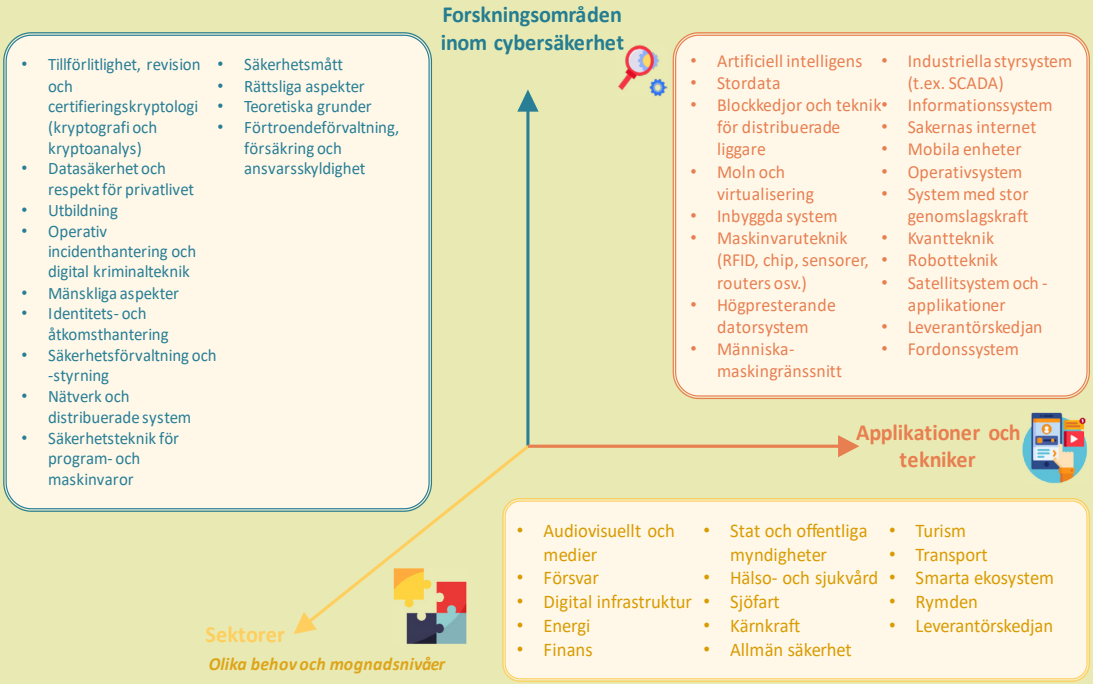
Ruta 5

Försök att prata samma cyberspråk: *teknisk samstämmighet*

Terminologisk klarhet förbättrar situationsmedvetenheten och samordningen[143] och bidrar till att exakt fastställa vad som utgör ett hot och en risk.

Kommissionens gemensamma forskningscentrum (JRC) har nyligen tagit fram en omarbetad forskningstaxonomi med utgångspunkt i olika internationella standarder[144]. Tanken är att den ska bli en referenspunkt som kan användas som ett index av forskningsorganisationer i hela Europa.

Taxonomi för cybersäkerhet



Källa: Revisionsrätten, anpassade uppgifter från Europeiska kommissionen.

Fram till nyligen hade inte EU:s institutioner och byråer några gemensamma definitioner. Det håller på att ändras. Inom ramen för sin plan utformade samarbetsgruppen en incident-taxonomi i syfte att underlätta effektivt gränsöverskridande samarbete.

Samarbete och informationsutbyte med den privata sektorn

97 Samarbete mellan offentliga myndigheter och den privata sektorn är avgörande för att stärka de övergripande cybersäkerhetsnivåerna. Trots det fann kommissionen i sin utvärdering av strategin för cybersäkerhet från 2017 att informationsutbytet mellan privata aktörer och mellan offentlig och privat sektor ännu inte var optimalt på grund av att det saknades tillförlitliga rapporteringsmekanismer och incitament för att dela information[145], vilket gjorde det svårt att uppnå strategiska mål. Kommissionen har också noterat att det saknas en effektiv samarbetsmekanism som möjliggör för medlemsstaterna att samarbeta för att strategiskt förbättra långsiktig industriell kapacitet i stor skala[146].

98 Informations- och analyscentraler är organisationer som har inrättats för att tillhandahålla plattformar och resurser för att underlätta informationsutbyte mellan den offentliga och den privata sektorn samt informationsinhämtning om cyberhot. De syftar till att skapa tillit genom att dela erfarenhet, kunskap och analys, i synnerhet om grundläggande orsaker, incidenter och hot. Nationella och sektoriella informations- och analyscentraler finns redan i ett antal medlemsstater, men på EU-nivå är antalet fortfarande begränsat[147]. Dock medför de ett antal utmaningar (begränsade resurser och svårigheter när det gäller att utvärdera hur framgångsrika de är, att säkerställa rätt strukturer för att engagera både offentlig och privat sektor och att involvera rättsvårdande myndigheter) som måste överbryggas om de ska kunna bidra till att genomföra NIS-direktivet och bygga upp säkerhetskapacitet på en EU-omfattande nivå[148].

99 Nära samarbete med den privata sektorn är särskilt avgörande för att bekämpa komplex it-brottslighet, men effektiviteten varierar mellan medlemsstaterna och beror på tillitsnivån[149]. Europols EC3 har dock inrättat ett antal rådgivande grupper med aktörer från den privata sektorn, EU:s institutioner och byråer samt andra internationella organisationer för att förbättra samarbetet genom nätverkande, strategiskt underrättelseutbyte och samarbete. De arbetar enligt planer i linje med målen för EU:s policycykel[150]. Brottsligt missbruk av kryptering är ett annat område där det finns många utmaningar som kräver mer samarbete med den privata sektorn. Europols EC3 undersöker just nu möjligheter att förmedla fallspecifikt kortsiktigt deltagande i J-CAT (se punkt ***62***) för experter från den privata sektorn och den akademiska världen.

100 Avsaknaden av effektiva samarbetsmekanismer utgör ett problem för både civilsamhället och försvaret – både det offentliga och det privata. Bland de områden

som ofta utgör utmaningar återfinns kryptering, säkra inbyggda system, upptäckt av sabotageprogram, simuleringstekniker, skydd av nätverks- och systemkommunikation samt autentiseringstekniker. Att främja civilt-militärt samarbete och stödja forskning och teknik (i synnerhet genom att stödja små och medelstora företag) är två av prioriteringarna i den uppdaterade ramen för EU:s politik för it-försvar (uppdatering 2018).

Reflektionspunkter – bygga upp resiliens

- Hur kan en lämplig balans uppnås på EU-nivå mellan behovet av att integrera cybersäkerhetspolitiken och säkerställa effektiv samordning mellan olika aktörer och fördelning av ansvar?
- Hur väl förberedda är EU:s institutioner och byråer på nästa stora angrepp direkt mot dem?
- Hur kan EU:s cyberrelevanta byråer bli attraktivare för talanger?
- Vilka ytterligare steg krävs för att säkerställa lämplig kapacitet i alla EU:s institutioner och byråer för att möjliggöra en konsekvent ram för risk- och hotbedömning?
- På vilka sätt hanterar de europeiska tillsynsmyndigheterna (Europeiska bankmyndigheten, Europeiska värdepappers- och marknadsmyndigheten och Europeiska försäkrings- och tjänstepensionsmyndigheten) de inneboende it-säkerhetsbristerna i finanssektorn och vad kan andra sektorer lära sig av detta?
- Mot bakgrund av bristen på expertis, hur kan EU:s tekniska bistånd för offentliga myndigheter bäst utnyttjas för att på ett övergripande sätt förbättra cyberresiliensen?
- Hur kan EU och medlemsstaterna säkerställa en meningsfull närvaro i internationella diskussioner för att påverka utformningen av cyberrymdens styrning och standarder och främja EU:s värden?
- Vilka åtgärder på EU-nivå och medlemsstatsnivå för att öka medvetenheten (inbegripet förebyggande åtgärder) gör verkligen skillnad och vad kan EU göra för att bygga ut dem?
- Vilken roll spelar EU i att bidra till att jämna ut könsfördelningen på cybersäkerhetsområdet?
- Hur kan EU och medlemsstaterna förbättra synergieffekterna mellan civilsamhället och försvaret, i linje med ramen för politiken för it-försvar (uppdatering 2018)?

Hantera cyberincidenter ändamålsenligt

101 Att hitta ett ändamålsenligt sätt att hantera cyberangrepp är avgörande för att stoppa dem så tidigt som möjligt. Det är särskilt viktigt att kritiska sektorer, medlemsstater och EU-institutioner kan svara på ett snabbt och samordnat sätt. Tidig detektering är avgörande.

Utmaning 9: ändamålsenlig detektering och hantering

Detektering och rapportering

102 Vanliga detekteringsverktyg bidrar till att bekämpa de flesta angrepp som sker varje dag[151]. Dock har de digitala systemen blivit så komplexa att det är omöjligt att förhindra alla angrepp. Eftersom de är så sofistikerade undgår de ofta att bli upptäckta under längre perioder. Experter menar därför att fokus bör ligga på snabb detektering och hantering[152]. Dock är det få företag som använder detekteringsverktyg som bygger på till exempel automatisering, maskininlärning och beteendeanalys och som syftar till att minska riskerna och analysera och lära från systemets beteende[153]. Detta beror delvis på att falska positiva resultat genereras, vilket leder till att aktiviteter som inte utgör hot misstas som illvilliga.

103 När en överträdelse har detekterats och analyserats krävs snabb rapportering så att andra offentliga och privata enheter kan vidta förberedande åtgärder och så att relevanta myndigheter kan stödja dem som påverkats. Många organisationer tvekar att tillstå och rapportera cyberincidenter[154]. Det är också avgörande att redan tidigt involvera rättsvårdande myndigheter i den inledande hanteringen av misstänkt it-brottslighet och att proaktivt utbyta information med CSIRT-enheterna.

104 Den tidigare bristen på gemensamma EU-krav på incidentrapportering riskerade att fördröja rapporteringen av överträdelser och förhindra hanteringen, vilket införandet av NIS-direktivet avsåg att åtgärda (se punkt ***20***). Efter Wannacry-angreppen 2017 drog kommissionen slutsatsen att CSIRT-nätverkssystemet fortfarande inte fungerade fullt ut[155]. I takt med att genomförandet av direktivet fortsätter återstår det att se huruvida de riktlinjer som samarbetsgruppen har utarbetat kan bidra till att minska motviljan att rapportera incidenter[156].

105 Leverantörer av samhällsviktiga tjänster i vissa sektorer har flera rapporteringsskyldigheter (inbegripet till konsumenter) inom ramen för befintliga EU-förordningar, vilket kan påverka processens effektivitet. Till exempel är leverantörer i finans- och banksektorn föremål för olika rapporteringskriterier, standarder, tröskelvärden och tidsfrister inom ramen för GDPR, NIS-direktivet, betaltjänstdirektivet, Europeiska centralbanken/gemensamma tillsynsmekanismen, Target 2 och eIDA-förordningen[157]. Det är därför viktigt att samordna dessa skyldigheter eftersom heterogeniteten kan leda till fragmenterad rapportering, förutom att den utgör en onödig administrativ börda.

Samordnad hantering

106 Utvecklingen av en ram för europeiskt samarbete vid en cybersäkerhetskris är fortfarande ett pågående arbete. Den tillhörande planen[158] (se punkt ***18***) infördes därför för att ingjuta ett cyberperspektiv i IPCR-mekanismen (integrerad politisk krishantering), förbättra situationsmedvetenheten och säkerställa bättre integrering med andra EU-mekanismer för krishantering[159]. Planen inbegriper EU:s institutioner och byråer samt medlemsstaterna. Det är utmanande att sömlöst integrera alla dessa krishanteringsmekanismer[160]. Den nuvarande bristen på ett gemensamt säkert kommunikationsnätverk för alla EU-institutioner är också en viktig brist[161].

107 EU:s förmåga att hantera cyberangrepp på operativ och politisk nivå vid en storskalig, gränsöverskridande incident har betecknats som begränsad, delvis eftersom cybersäkerhet fortfarande inte har integrerats i befintliga samordningsmekanismer för krishantering på EU-nivå[162]. Detta tas inte upp i NIS-direktivet.

108 Den nyligen föreslagna reformen av Enisa, som förutsåg en större operativ roll i hantering av storskaliga cybersäkerhetsincidenter, stöddes inte av medlemsstaterna, som hellre såg att byråns roll skulle stödja och komplettera deras egna operativa åtgärder[163]. Det finns redan många CERT/CSIRT-enheter på medlemsstatsnivå, men deras kapacitet varierar avsevärt. Det här utgör ett hot mot det ändamålsenliga gränsöverskridande samarbete som krävs för storskalig incidenthantering[164].

109 Vi försökte kartlägga de olika roller som tilldelats de olika aktörer som identifierats i planen, men det fanns luckor som måste fyllas i takt med att genomförandet fortskrider. Ett område som inledningsvis inte berördes tillräckligt var brottsbekämpning, trots att EU:s beredskapsprotokoll för brottsbekämpning började gälla i december 2018[165]. Det är avgörande för planens framgång att den är praktisk

och att alla parter vet vad de ska göra. Detta kräver omfattande tester under de kommande åren.

110 Ändamålsenlig hantering handlar om mer än skadereducering. Det är också avgörande att tillskriva ansvar för angrepp. Det kan vara väldigt svårt att spåra och identifiera förövare, särskilt i ett hybridangrepp, på grund av det växande missbruket av anonymiseringsverktyg, kryptovalutor och kryptering. Detta kallas för tillskrivningsproblemet. Att komma till rätta med det här problemet är inte bara en teknisk fråga, utan också en straffrättslig utmaning. Rättsliga och förfarandemässiga skillnader mellan länder kan påverka rättsliga utredningar och lagföring av misstänkta. För att hantera tillskrivningsproblemet krävs till exempel ett mer formaliserat operativt informationsutbyte genom tydligare förfaranden med Europol eller Eurojusts europeiska rättsliga nätverk mot it-brottslighet.

111 På politisk nivå har verktygslådan för cyberdiplomati (se ***ruta 6***) utvecklats i syfte att stödja fredlig internationell tvistlösning i cyberrymden. Inrättandet av snabbinsatsteam och ett initiativ för ömsesidigt bistånd på området för cybersäkerhet är två projekt som främjar förbättrat informationsutbyte och som utvecklas inom ramen för Pesco[166].

Ruta 6

Verktygslådan för cyberdiplomati

En gemensam diplomatisk respons från EU mot skadlig it-verksamhet[167], eller ”verktygslådan för cyberdiplomati”, växte fram ur rådets slutsatser om cyberdiplomati från 2015[168]. Cyberdiplomati syftar till att utveckla och genomföra en gemensam och heltäckande strategi för cyberrymden baserat på EU:s värden, rättsstatsprincipen, kapacitetsuppbyggnad och partnerskap, främjande av flerpartsmodellen för förvaltning av internet, begränsning av cybersäkerhetshot och ökad stabilitet i internationella relationer.

Verktygslådan möjliggör för EU och medlemsstaterna att utforma en gemensam diplomatisk respons mot skadlig it-verksamhet som fullt ut utnyttjar åtgärderna inom den gemensamma utrikes- och säkerhetspolitiken. Det kan handla om förebyggande åtgärder (t.ex. ökad medvetenhet, kapacitetsuppbyggnad), åtgärder som främjar samarbete och stabilitet samt begränsande åtgärder (t.ex. reseförbud, vapenembargon, fryst finansiering) eller stöd till medlemsstaternas respons mot skadlig it-verksamhet[169]. Tanken är att ytterligare samarbete för att minska hot och tydligt signalera de troliga konsekvenserna av gemensam hantering (eventuellt) kan avskräcka från aggressivt beteende.

EU:s gemensamma hantering av skadlig it-verksamhet kommer att vara proportionerlig när det gäller it-verksamhetens räckvidd, skala, tidslängd, intensitet, komplexitet, finess och inverkan.

Avgörande för verktygslådans framgång är hur väl den integreras i planen och IPCR (se punkt ***106***), hur väl situationsmedvetenhet upprättas genom snabbt och kontinuerligt informationsutbyte (inbegripet om tillskrivningselement)[170] och slutligen ändamålsenligt samarbete. Ändamålsenlig och samordnad kommunikation är också viktig för att verktygslådan ska kunna tillämpas framgångsrikt. Hittills har verktygslådan använts två gånger: för att inleda en dialog med Förenta staterna efter *Wannacry*-angreppet[171] och för att utveckla slutsatser från rådet som fördömer missbruk av IKT[172]. Det operativa genomförandet av verktygslådan pågår och det återstår att se hur ändamålsenlig den är när det gäller att uppnå målen.

Utmaning 10: skydda kritisk infrastruktur och kritiska samhällsfunktioner

Skydda infrastruktur

112 En stor del av EU:s kritiska infrastruktur drivs genom industriella styrsystem[173]. Många av dessa utformades som autonoma system med begränsad koppling till världen utanför. När komponenter i de industriella styrsystemen har anslutits till internet har de blivit känsligare för intrång utifrån. Underhåll och reparation av befintliga system kanske inte längre är möjligt, och att uppgradera dem är inte billigt och går inte snabbt. Insatserna för att förbättra säkerheten i kritisk infrastruktur måste därför inbegripa uppgradering av de industriella styrsystemen.

113 I takt med att industrin fortsätter att digitaliseras (kallas vanligen ”Industri 4.0”) kan påverkan från en storskalig incident i en industrisektor ha indirekta återverkningar på andra ställen. Enisa har noterat vikten av att kartlägga påverkan från kritiska sektorers ömsesidiga beroenden[174]. Det här är avgörande för att förstå hur en incident eventuellt kan spridas och ligger till grund för väl samordnad hantering.

114 NIS-direktivet syftar till att förbättra beredskapen i viktiga sektorer som ansvarar för kritisk infrastruktur. Dock omfattas inte alla sektorer (se ***tabell 1***)[175], vilket minskar strategins ändamålsenlighet[176]. Ett stort bekymmer är att skydda valens demokratiska integritet från inblandning i valinfrastrukturen och desinformation (se ***ruta 7***). Förutom att se över den befintliga lagstiftningen är därför en viktig

utmaning att undersöka hur dessa sektorer kan involveras i ändamålsenlig hantering av storskaliga incidenter.

115 Säkerhetsbristerna i kritisk infrastruktur upphör inte vid Europas gränser. En särskild utmaning för kommissionen är att uppmuntra kandidatländerna att anta samma standarder som medlemsstaterna, till exempel på områden såsom cyberrelaterad lagstiftning eller skydd av kritisk infrastruktur.

Ruta 7

Skydda kritiska samhällsfunktioner: *bekämpa inblandning i val*

I maj 2019 kommer omkring 400 miljoner väljare att gå till röstlokalerna i valet till Europaparlamentet, det första som sker inom ramen för GDPR. Valet sker i kölvattnet av de skandaler som omger missbruket av personuppgifter för politisk microtargeting och samordnade desinformationskampanjer (”falska nyheter”) som saknat motstycke. Kommissionen har varnat för att cyberinblandning i valet är sannolikt[177], och att bekämpa detta kräver ett tillvägagångssätt som inbegriper hela statsförvaltningen och hela samhället.

Valinfrastruktur

Det är komplext att organisera val och det är medlemsstaternas ansvar att säkerställa deras skydd och integritet. Inblandning i val och valinfrastruktur kan syfta till att påverka väljarnas preferenser, valdeltagandet eller själva valprocessen, inbegripet den faktiska röstningen samt rösträkning och rapportering. I valet till Europaparlamentet är det en särskilt viktig utmaning att skydda den så kallade ”sista kilometern” (rapporteringen av resultat från de nationella huvudstäderna till Bryssel), mot bakgrund av att någon gemensam säkerhetsstrategi inte finns eller har testats[178].

Kommissionens senaste valpaket innefattade åtgärder för att stärka cybersäkerheten för val. Till exempel utsågs nationella kontaktpunkter för att samordna och utbyta information inför valet. Utbyte av bästa praxis och lärdomar är extra viktigt[179].

Valsystem anses inte ingå i kritisk infrastruktur[180] och de omfattas inte heller av NIS-direktivet. Trots det har samarbetsgruppen utvecklat en praktisk vägledning om säkerhet för valteknik till stöd för offentliga myndigheter. De nationella kontaktpunkterna förväntas sammanträda i början av 2019[181]. Medlemsstaterna uppmanas också att göra riskbedömningar av cyberhot mot sina valprocesser.

Desinformation

Desinformation är ett allt viktigare element i hybridangrepp som inbegriper cyberangrepp och hackning av nätverk. Syftet kan vara att dela samhällen, skapa misstro och undergräva förtroendet för demokratiska processer eller andra frågor (till exempel antivaccination eller klimatförändringar). Problemet har ökat i skala, hastighet och omfattning och utgör ett genuint säkerhetshot mot EU.

EU har vidtagit ett antal åtgärder för att bekämpa desinformation. År 2015 inrättades arbetsgruppen East Stratcom inom Europeiska utrikestjänsten för att bekämpa ryska desinformationskampanjer[182]. Experter har hyllat dess arbete med att främja EU:s politik, stödja oberoende medier i grannskapet samt göra prognoser för, följa upp och hantera desinformation[183]. Dock är arbetsgruppens resurser begränsade i förhållande till desinformationskampanjernas skala och komplexitet[184]. Ett mer systematiskt samspel med befintliga EU-strukturer och ett förbättrat samarbete för strategisk kommunikation krävs.[185] En ny åtgärdsplan[186] godkändes av Europeiska rådet i december 2018.

På senare tid har kommissionen, mot bakgrund av sitt meddelande om att bekämpa desinformation online från april 2018[187], utvecklat en frivillig, självreglerande uppförandekod[188], baserad på befintliga politiska instrument, som onlineplattformar och reklambranschen har undertecknat[189]. Åtgärderna består bland annat av att bidra till att öka innehållets tillförlitlighet och stödja insatser för att öka medie- och nyhetskompetens. Ett oberoende europeiskt faktagranskarnätverk har också startats.

Kommissionen har angett att ytterligare lagstiftningsåtgärder kan följa om uppförandekoden inte beaktas. Det kommer att vara av avgörande vikt att fastställa åtgärdernas ändamålsenlighet, i synnerhet genom att avgöra hur förbättringar av tillit, transparens och ansvarstagande ska mätas.

En annan utmaning blir att hitta sätt att förbättra detektering, analys och avslöjande av desinformation[190]. Aktiv och strategisk övervakning och analys av öppna datakällor behövs också[191]. Försök att få en bättre förståelse av hotmiljön bör också omfatta framväxande tendenser, till exempel ”deepfakes” (falska videor som är gjorda med hjälp av artificiell intelligens och djup maskininlärning) och sluten kryptering, samt de verktyg som krävs för att upptäcka dem.

Förbättra autonomin

116 EU är en nettoimportör av produkter och tjänster som rör cybersäkerhet, vilket ökar risken för tekniskt beroende av, och sårbarhet för, operatörer utanför EU[192]. I synnerhet är det här en realitet som undergräver säkerheten i EU:s kritiska infrastruktur, som också stöds av komplexa globala leveranskedjor. Risken förvärras

ytterligare om operatörer utanför EU förvärvar europeiska cybersäkerhetsföretag. Medlemsstaterna ansvarar för att granska utländska direktinvesteringar och för närvarande finns det inte någon EU-omfattande granskningsmekanism[193].

117 Större strategisk autonomi är ett mål i EU:s globala strategi och meddelandet *Resiliens, avskräckning och försvar*[194] från 2017. En hantering av det stora antalet utmaningar i den här rapporten skulle bidra till att förbättra den här autonomin. Det finns ingen enskild åtgärd som ensamt uppnår detta.

Reflektionspunkter – ändamålsenlig hantering

- Hur har NIS-direktivet förbättrat rapporteringen av cyberincidenter i kritiska sektorer och andra sektorer?
- Hur väl internaliserar EU:s institutioner samordning av krishantering för en stor cyberincident?
- Hur kan cyberdiplomati spela en mer framträdande roll i EU:s yttre åtgärder?
- Är EU:s nuvarande strukturer och åtgärder för att bekämpa desinformation proportionerliga till problemets skala och komplexitet?

Avslutande kommentarer

118 På senare år har EU och medlemsstaterna prioriterat upp cybersäkerhet på agendan i syfte att förbättra den övergripande cyberresiliensen. Trots det är det ett stort projekt att uppnå en högre cybersäkerhetsnivå i unionen. I det här briefingdokumentet har vi försökt lyfta fram några av de främsta utmaningarna för EU:s ambition att bli världens säkraste digitala miljö.

119 Vår granskning visar att det krävs en övergång till en resultatkultur med inbyggda utvärderingsmetoder för att säkerställa **meningsfullt ansvarstagande och meningsfull utvärdering**. Vissa **luckor i lagstiftningen finns kvar och den befintliga lagstiftningen har inte införlivats konsekvent av medlemsstaterna**. Det kan göra det svårt att utnyttja lagstiftningen fullt ut. En annan identifierad utmaning rör **anpassning av investeringsnivåerna till de strategiska målen**, vilket kräver ökade investeringar och ökad effektivitet. Det här är mer krävande om EU och medlemsstaterna inte har en **tydlig översikt över EU:s utgifter** för cybersäkerhet. Det har också rapporterats om **begränsade resurser för EU:s byråer med cyberrelaterad verksamhet,** inbegripet svårigheter att attrahera och behålla talanger.

120 I tillgängliga studier dras slutsatsen att **styrningen av cybersäkerheten kan stärkas** för att främja det globala samfundets förmåga att hantera cyberangrepp och -incidenter. Samtidigt är det omöjligt att förhindra alla angrepp. Viktiga utmaningar som måste hanteras är därför **snabb detektering och hantering** och **skydd av kritisk infrastruktur och kritiska samhällsfunktioner** samt bättre **utbyte och samordning av information** mellan den offentliga och den privata sektorn. Slutligen innebär den växande globala kompetensbristen inom cybersäkerhet att det också är en viktig utmaning att **öka kompetensen och medvetenheten** i alla sektorer och på alla samhällsnivåer.

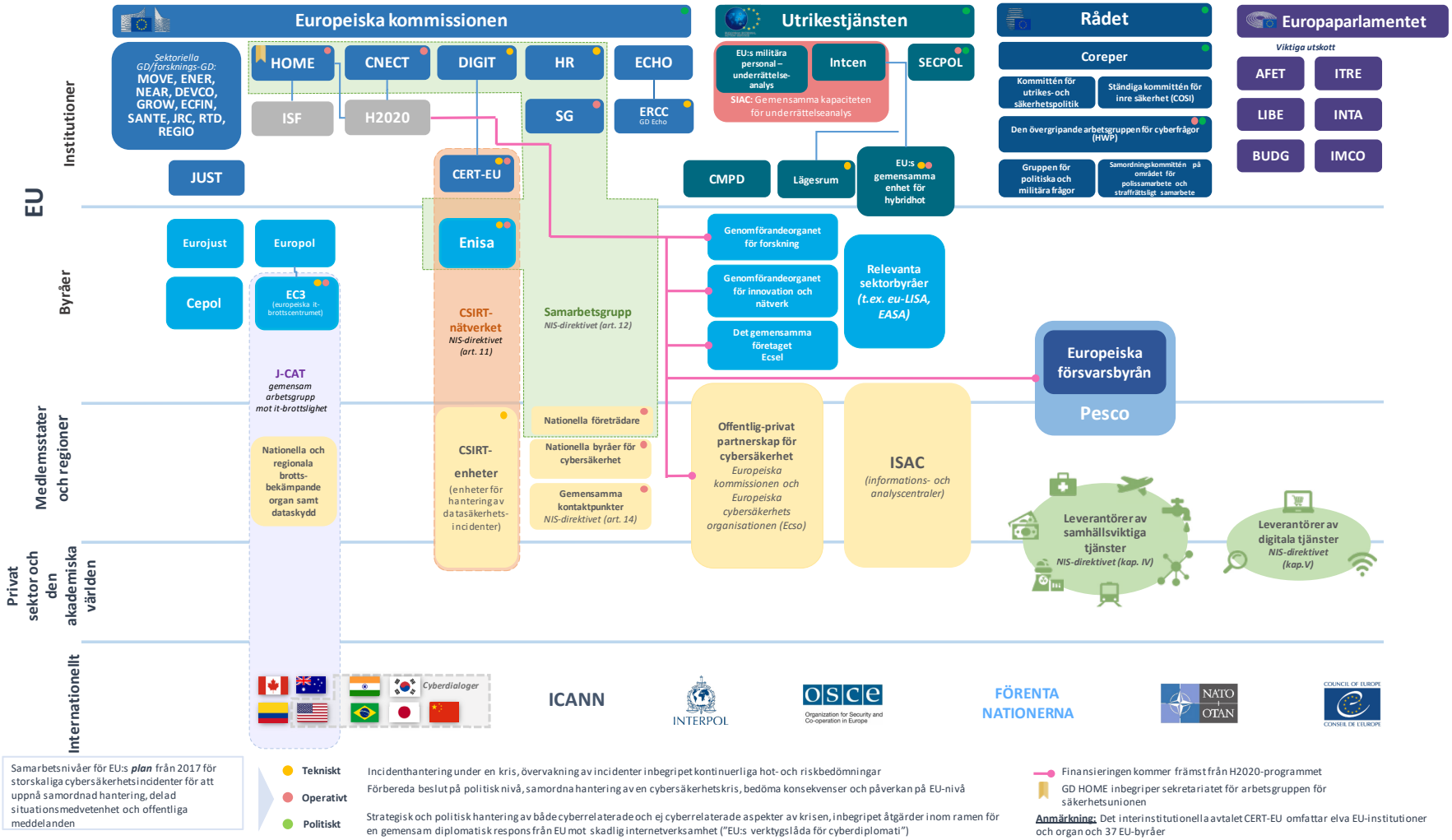
121 Utmaningarna med cyberhot mot EU och hela den globala miljön kräver ett kontinuerligt engagemang och att vi orubbligt står fast vid EU:s värden.

Detta briefingdokument antogs av avdelning III vid dess sammanträde den 14 februari 2019.

För revisionsrätten

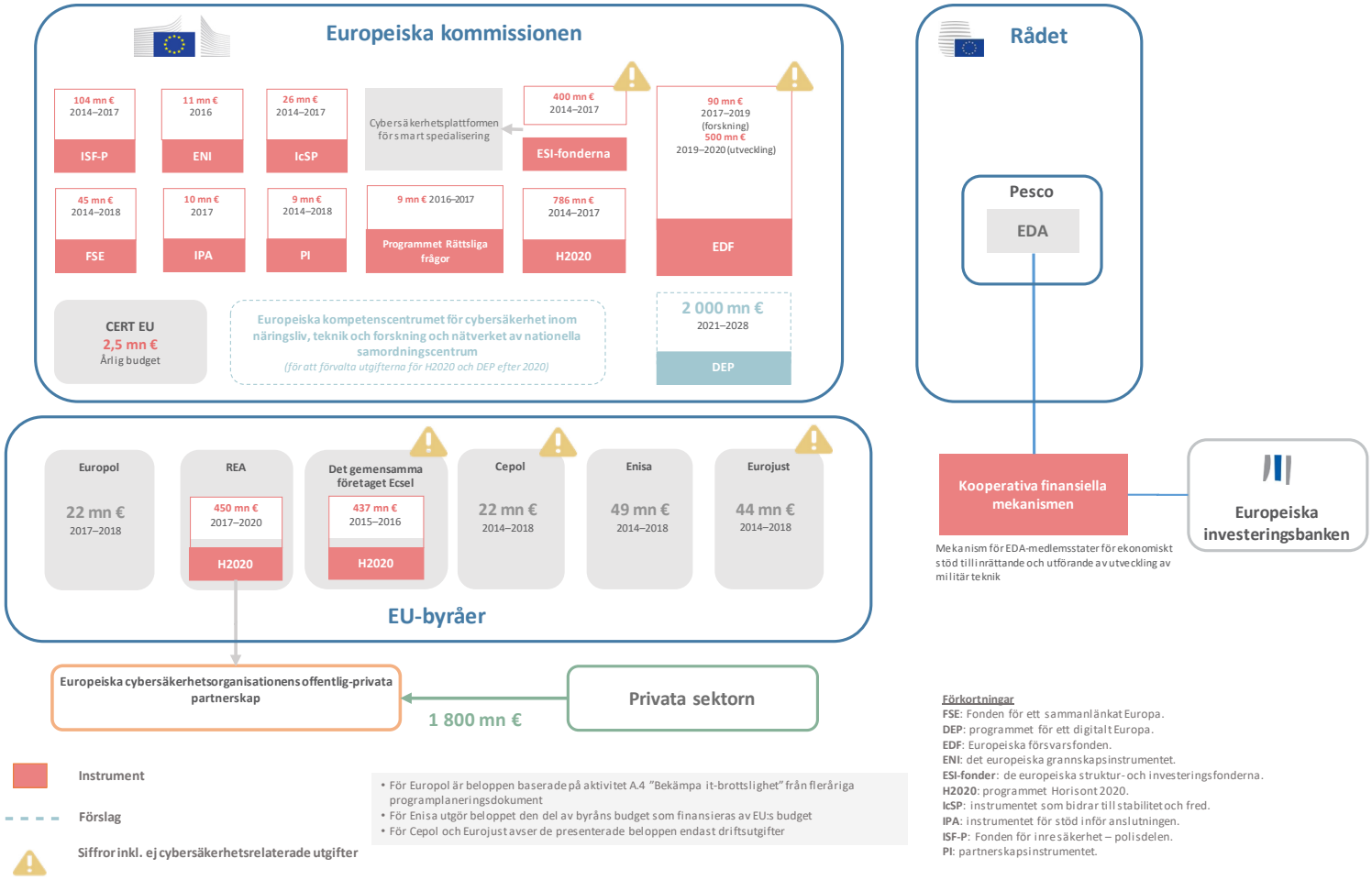
Klaus-Heiner Lehne
Ordförande

Bilaga I — Ett komplext landskap i flera skikt med många aktörer



Källa: Revisionsrätten.

Bilaga II — EU:s utgifter för cybersäkerhet sedan 2014



Källa: Revisionsrätten, baserat på dokument från Europeiska kommissionen och EU-byråer.

Bilaga III — Rapporter från revisionsorganen i EU:s medlemsstater

Typ	Titel (med länk)	År	MS
Regelefterlevnadsrevisioner	Anmärkning angående internkontrollbedömning	2014	FR
	Attesteringsrapport för det allmänna socialförsäkringssystemets räkenskaper (försvar, utrikes frågor)	2016	FR
	Attestering av de statliga räkenskaperna	2016	FR
	Säkerställa säkerhet och bevarande av estniska nationella databaser av stor vikt	Klar 2018/inte offentliggjord än	EE
	Internkontrollernas ändamålsenlighet i skyddet av personuppgifter i nationella databaser	2008	EE
Effektivitetsrevisioner	Rapport om förebyggande av cyberangrepp	2013	DK
	RiR 2014:23 Informationssäkerheten i den civila statsförvaltningen	2014	SE
	Rapport om regeringens behandling av konfidentiella uppgifter om personer och företag	2014	DK
	Nationella cybersäkerhetsprogrammet	2014	UK
	Rapport till förbundsdagens budgetkommitté i enlighet med § 88.2 i den federala budgetlagen (BHO) – it-konsolidering, den federala regeringen	2015	DE
	Rapport om åtkomst till it-system som stöder leveransen av samhällsviktiga tjänster i Danmark	2015	DK
	Plaine de Frances myndighet för offentlig planering	2015	FR
	Cybersäkerhetsmiljön i Litauen en version på litauiska en sammanfattning översatt till engelska	2015	LT
	Offentliga organs utförande av cybersäkerhetsuppgifter i Polen (på polska)	2015	PL
	RiR 2015:21 It-relaterad brottslighet – polis och åklagare kan bli effektivare	2015	SE
	Det digitala kompetensunderskottet i regeringen (enkät)	2015	UK
	Rapport till det federala parlamentet: Federala finanser: insamling av arvsskatt	2016	BE
	Rapport om hantering av it-säkerhet i system som lagts ut på entreprenad till externa leverantörer	2016	DK
	Granskningsrapport avseende det officiella kreditinstitutets låneverksamhet 2016	2016	ES
	Styrning av förvaltningens säkerhetsnätsverksamhet	2016	FI
	Säkerställa säkerheten i it-system som används för offentliga uppgifter	2016	PL
	Förebygga och bekämpa nätmobbning bland barn och ungdomar	2016	PL

Typ	Titel (med länk)	År	MS
	Informationssäkerhetsarbete på nio myndigheter – En andra granskning av informationssäkerhet i staten. RiR 2016:8	2016	SE
	Skydda information i regeringen	2016	UK
	Rapport om skyddet av it-system och hälsouppgifter i tre danska regioner	2017	DK
	Anmärkning angående resultaten av den internationella parallellrevisionen ”Internkontrollernas ändamålsenlighet i skyddet av personuppgifter i nationella databaser”.	2017	EE
	Organisering av cyberskyddet	2017	FI
	Styrning av funktionssäkerheten i e-tjänster	2017	FI
	Jordbrukskammarens nätverk (sammanfattning)	2017	FR
	Vaucluses handels- och industrikammare (från den regionala revisionskammaren PACA)	2017	FR
	Säkerställa säkerhet och bevarande av estniska nationella databaser av stor vikt	Klar 2018/inte offentliggjord än	EE
	Infrastrukturutveckling av statens elektroniska kommunikationer en version på litauiska en sammanfattning översatt till engelska	2017	LT
	Revision av informationsteknik: cybersäkerhet i alla offentliga organ	2017	MT
	Det nationella registersystemet: säkerhet, prestanda och användbarhet	2017	PL
	WannaCry-incidenten	2017	UK
	Nätbedrägerier	2017	UK
	Rapport om skydd mot angrepp från utpressningstrojaner	2018	DK
	Arpajon-sjukhuset (från den regionala kammaren i Île-de-France)	2018	FR
	Hantering av kritiska statliga informationsresurser	2018	LT
	Elektroniska brott	2019	LT
	Finns det förutsättningar för ändamålsenligt skydd av Lettlands cyberrymd?	2019	LV
	Informationssäkerhet i Polen	2019	PL
Övrigt	Databas över offentliga organ	–	BE
	Frågeformulär om säkerhets- och riskanalyspolitik (pågående)	–	BE

Akronymer och förkortningar

CERT-EU: incidenthanteringsorganisationen för EU:s institutioner och byråer.

CSIRT: it-incidentcentrum (enhet för hantering av it-säkerhetsincidenter).

DDoS: samordnad överbelastning (Distributed Denial of Services).

DEP: programmet för ett digitalt Europa.

DIGIT: kommissionens generaldirektorat för informationsteknik.

EC3: Europols europeiska it-brottscentrum.

Ecsel: det gemensamma företaget för elektroniska komponenter och system för europeiskt ledarskap.

ECSM: den europeiska månaden för it-säkerhet.

Ecso: Europeiska cybersäkerhetsorganisationen.

EDA: Europeiska försvarsbyrån.

Enisa: Europeiska unionens byrå för nät- och informationssäkerhet.

ESA: den europeiska tillsynsmyndigheten.

ESI-fonder: europeiska struktur- och investeringsfonder.

EU: Europeiska unionen.

GD CNECT: kommissionens generaldirektorat för kommunikationsnät, innehåll och teknik.

GD HOME: kommissionens generaldirektorat för migration och inrikes frågor.

GD JUST: kommissionens generaldirektorat för rättsliga frågor och konsumentfrågor.

GDPR: den allmänna dataskyddsförordningen.

GSFP: EU:s gemensamma säkerhets- och försvarspolitik.

ISF - P: Fonden för inre säkerhet – polisdelen.

ISSB: styrelsen för informationssäkerhet.

JRC: gemensamma forskningscentrumet.

LISO: säkerhetsansvarig för de lokala datasystemen.

NCIRC: Natos it-incidenthanteringsorgan.

NIS-direktivet: direktivet om nät- och informationssäkerhet.

Pesco: permanent strukturerat samarbete.

SMF: små och medelstora företag.

Ordförklaringar

befintliga system: datorsystem, applikationer eller programmeringsspråk som är föråldrade eller omoderna och fortfarande används, men som eventuellt saknar uppgraderingar och försäljningsstöd, inbegripet säkerhetssupport.

betrodda tjänster: tjänster som förbättrar en elektronisk transaktions rättsliga giltighet, såsom elektroniska underskrifter, stämplar, tidsstämplingar, rekommenderade leveranser och autentisering av webbplatser.

botnät: ett nätverk av datorer som är infekterade med sabotageprogram och fjärrstyrs, utan användarens vetskap, för att skicka skräppost, stjäla information eller inleda samordnade cyberangrepp.

brott som nättjänst-modellen: en brottslig affärsmodell som driver den digitala underjordiska ekonomin och tillhandahåller ett stort utbud av kommersiella tjänster och verktyg som möjliggör för it-brottslingar utan någon särskild kompetens att begå it-brott.

cyberangrepp: ett försök att undergräva eller förstöra uppgifters eller ett datorsystems konfidentialitet, integritet och tillgänglighet genom cyberrymden.

cyberekosystem: ett komplext landskap av interagerande enheter, uppgifter, nätverk, människor, processer och organisationer samt processernas och teknikernas miljö som påverkar och stöder dessa interaktioner.

cyberincident: en händelse som direkt eller indirekt skadar eller hotar resiliens och säkerhet för ett it-system och de data som det behandlar, lagrar eller överför.

cyberresiliens: förmågan att förhindra, ha beredskap för, stå emot och återhämta sig från cyberangrepp och -incidenter.

cyberrymd: den ogreppbara globala miljö där onlinekommunikation sker mellan människor, programvaror och tjänster via datornätverk och tekniska enheter.

cybersäkerhet: alla skydd och åtgärder som införts för att försvara it-system och deras data mot obehörig åtkomst, angrepp och skada för att säkerställa deras tillgänglighet, konfidentialitet och integritet.

desinformation: verifierbart oriktiga eller missvisande uppgifter som skapas, presenteras och sprids för att uppnå ekonomisk vinning eller avsiktligt vilseleda allmänheten, och som kan orsaka skada för allmänheten.

digitalt innehåll: alla data – såsom text, ljud, bilder eller video – som lagras i digitalt format.

exploit kit: en slags verktygslåda som it-brottslingar använder för att angripa säkerhetsbrister i nätverk och informationssystem så att de kan distribuera sabotageprogram eller utföra annan skadlig verksamhet.

hacktivist: individ eller grupp som skaffar sig obehörig åtkomst till informationssystem eller nätverk i syfte att främja sociala eller politiska ändamål.

hantering av säkerhetsbrister: en integrerad del av dator- och nätverkssäkerhet för att proaktivt begränsa eller förhindra utnyttjande av säkerhetsbrister i system- och programvaror genom att identifiera, klassificera och åtgärda dem.

hybridhot: fientlig avsikt som en motpart ger uttryck för med hjälp av en blandning av konventionella och icke-konventionella krigföringstekniker (dvs. militära, politiska, ekonomiska och tekniska metoder) för att med kraft eftersträva sina mål.

informationssäkerhet: en uppsättning processer och verktyg som skyddar fysiska och digitala data från obehörig åtkomst, användning, röjande, störning, ändring, registrering eller förstörelse.

integritet: skydd mot otillbörlig ändring eller förstörelse av information och garanti för dess äkthet.

it-baserad brottslighet: ett traditionellt brott som begås i större skala med hjälp av it-system.

it-beroende brottslighet: brottslighet som endast kan begås med it-enheter.

it-brottslighet: olika brottsliga aktiviteter som inbegriper datorer och it-system som antingen ett primärt verktyg eller ett primärt mål; dessa aktiviteter omfattar traditionella brott (t.ex. bedrägeri, förfalskning och identitetsstöld), innehållsrelaterade brott (t.ex. onlinedistribution av barnpornografi eller uppmaning till religiöst hat) och brott som är unika för datorer och informationssystem (t.ex. angrepp mot informationssystem, överbelastningsattacker och sabotageprogram).

it-försvar: underfunktion till cybersäkerhet som syftar till att försvara cyberrymden med militära och andra lämpliga åtgärder för att uppnå militära-strategiska mål.

konfidentialitet: skydd av information, data eller tillgångar från obehörig åtkomst eller röjande.

kortkapning: stöld av kredit- eller betalkortsdata när de anges online.

kritisk infrastruktur: fysiska resurser, tjänster och anläggningar som vid störningar eller förstörelse skulle påverka ekonomins och samhällets funktioner i stor utsträckning.

kryptering: omvandling av läsbar information till oläslig kod i skyddssyfte; för att läsa informationen måste användaren ha tillgång till en hemlig nyckel eller ett hemligt lösenord.

kryptovaluta: En digital tillgång som utfärdas och utbyts genom krypteringsteknik, oberoende av en centralbank; den accepteras som betalningsmedel bland medlemmar i en virtuell gemenskap.

minerat sabotageprogram: en sorts sabotageprogram som syftar till att rensa hårddisken på den angripna datorn.

molnteknik: leverans av it-resurser – till exempel lagring, datorkapacitet eller datautbyteskapacitet – via internet genom värdtjänster på fjärrservrar.

nätfiske: förfarandet att skicka e-postmeddelanden som utger sig för att komma från en tillförlitlig källa i syfte att lura mottagarna att klicka på illvilliga länkar eller dela personlig information.

nätverkssäkerhet: underfunktion till cybersäkerhet som skyddar data som skickas via enheter i samma nätverk för att säkerställa att informationen inte skärs av eller förändras.

personuppgifter: information som rör en individ som kan identifieras.

programfix: en uppsättning ändringar av en programvara för att uppdatera, reparera eller förbättra den, inbegripet åtgärdande av säkerhetsbrister.

reklamprogram: sabotageprogram som visar reklambanderoller eller popupfönster som innehåller kod som spårar offrets onlinebeteende.

sabotageprogram: ett datorprogram som har utformats för att skada en dator, en server eller ett nätverk.

sakernas internet: nätverk av vardagliga föremål försedda med elektronik, programvara och sensorer så att de kan kommunicera och utbyta data via internet.

samordnad överbelastning (DDoS): ett cyberangrepp som hindrar legitima användare från att komma åt en onlinetjänst eller -resurs genom att överbelasta den med fler anrop än den kan hantera.

social ingenjörskonst: inom informationssäkerhet innebär det psykologisk manipulering för att lura människor att utföra en åtgärd eller avslöja konfidentiell information.

textvektorisering: förfarandet att omvandla ord, meningar eller hela dokument till numeriska vektorer så att algoritmer för maskininlärning kan använda dem.

tillgänglighet: säkerställa snabb och tillförlitlig åtkomst till och användning av information.

utpressningstrojan: sabotageprogram som nekar offren åtkomst till ett datorsystem eller gör filer oläsliga, vanligen genom kryptering; angriparen utpressar sedan oftast offret genom att vägra återställa åtkomsten tills en lösesumma betalas.

valinfrastruktur: inbegriper it-system och databaser för kampanjer, känslig information om kandidater, väljarregistrering och hanteringssystem.

åtkomstuppgifter: information om en användares inloggnings- och utloggningsverksamhet för åtkomst till en tjänst, till exempel tid, datum och IP- adress.

[1] I förslaget till EU:s cybersäkerhetsakt definieras det som ”all verksamhet som är nödvändig för att skydda nät- och informationssystem, deras användare och berörda personer mot cyberhot”. Akten förväntas antas av Europaparlamentet och rådet i början av 2019.

[2] Europol, *Internet Organised Crime Threat Assessment 2017* (hotbildsbedömning avseende den organiserade brottsligheten 2017).

[3] Europeiska cybersäkerhetsorganisationen (Ecso), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (europeiska cybersäkerhetssektorns förslag till ett avtalsbaserat offentligt-privat partnerskap), juni 2016.

[4] Europaparlamentet, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (cybersäkerhet i och utanför Europeiska unionen: utforska hot och politiska åtgärder), studie för utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor, september 2015.

[5] Enisa, *ENISA Threat Landscape Report 2017* (Enisas rapport om hotbilder 2017), 18.1.2018.

[6] Europol, *Internet Organised Crime Threat Assessment 2018* (hotbildsbedömning avseende den organiserade brottsligheten 2018).

[7] Europol, *ibid.*, 2018.

[8] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (stulna idéer: ska cyberspionage få hålla Europa tillbaka i den globala kapplöpningen om industriell konkurrenskraft?), occasional paper nr 2/18, februari 2018.

[9] Europeiska kommissionen, ordförandens tal om tillståndet i unionen 2017.

[10] Europol, *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down* (världens största marknadsplats som säljer internetförlamande DDoS-attacker nedtagen), pressmeddelande, 25.4.2018.

[11] Europol, *Internet Organised Crime Threat Assessment 2017* (hotbildsbedömning avseende den organiserade brottsligheten 2017).

[12] Europeiska kommissionens faktablad om cybersäkerhet, september 2017.

[13] Kostnaderna kan inbegripa: förlorade intäkter, kostnader för att reparera skadade system, eventuella skulder för stulna tillgångar eller stulen information, kundlojalitetsincitament, högre försäkringspremier, ökade skyddskostnader (nya system, anställda, utbildning) och eventuell reglering av efterlevnadskostnader eller rättstvister.

[14] NTT Security, *Risk:Value 2018 Report* (rapport om risk och värde 2018).

[15] Utpressningstrojanen *Wannacry* utnyttjade säkerhetsbrister i ett Microsoft Windows-protokoll och möjliggjorde fjärråtkomst till alla datorer. Microsoft utfärdade en programfix efter att säkerhetsbristen upptäcktes. Dock hade hundratusentals datorer ännu inte uppdaterats och många av dem infekterades följaktligen. Källa: A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too* (håll Nordkorea ansvarigt för Wannacry – och NSA också), WIRED, 19.12.2017.

[16] Europeiska kommissionen, *Europeans' attitudes towards cybersecurity* (européernas attityder till cybersäkerhet), särskild Eurobarometer 464a, september 2017. En uppföljande undersökning ska enligt planerna offentliggöras i början av 2019.

[17] Budapestkonventionen är en bindande internationell riktlinje för länder som tar fram lagstiftning om it-brottslighet. Den tillhandahåller ett ramverk för internationellt samarbete mellan stater. Kommissionen, Europeiska unionens råd, Europol, Enisa och Eurojust representerar för närvarande EU.

[18] Europeiska kommissionen, *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd*, JOIN(2013) 1 final, 7.2.2013.

[19] Europeiska kommissionen, *Europeiska säkerhetsagendan*, COM(2015) 185 final, 28.4.2015.

[20] Europeiska kommissionen, *En strategi för en inre digital marknad i Europa*, COM(2015) 192 final, 6.5.2015.

[21] Europeiska utrikestjänsten, *Delade visioner, gemensamma åtgärder: Ett starkare Europa. En global strategi för Europeiska unionens utrikes- och säkerhetspolitik*, juni 2016.

[22] Centre for European Policy Studies, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (stärka EU:s it-försvarskapacitet – rapport från en CEPS-arbetsgrupp), november 2018.

[23] Sabotageprogrammet bakom angreppen med utpressningstrojanen Wannacry, som Förenta staterna, Förenade kungariket och Australien tillskrev Nordkorea, utvecklades och sparades ursprungligen av Förenta staternas nationella säkerhetsmyndighet för att utnyttja säkerhetsbrister i Windows. Källa: A. Greenberg, ibid., *WIRED*, 19.12.2017. Efter angreppen fördömde Microsoft det faktum att regeringar sparar säkerhetsbrister i programvaror och upprepade sitt krav på en digital Genèvekonvention.

[24] Utöver land, hav, luft och rymden.

[25] Ram för EU:s politik för it-försvar (uppdatering 2018), 14413/18, 19.11.2018.

[26] Europeiska kommissionen/Europeiska utrikestjänsten, *Gemensam ram för att motverka hybridhot – Europeiska unionens insatser*, JOIN(2016) 18 final, 6.4.2016.

[27] Gemensam förklaring från Europeiska rådets ordförande, Europeiska kommissionens ordförande och Nordatlantiska fördragsorganisationens generalsekreterare, 8.7.2016 och 10.7.2018.

[28] Europeiska kommissionen/Europeiska utrikestjänsten, *Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*, JOIN(2017) 450 final, 13.9.2017.

[29] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

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

[31] Dessa är integrerade i kooperativa strukturer som inrättas genom direktivet, CSIRT-nätverket (ett nätverk bestående av EU-medlemsstaternas utsedda CSIRT-enheter och CERT-EU och vars sekretariat förvaltas av Enisa) och samarbetsgruppen (som stöder och underlättar det strategiska samarbetet och informationsutbytet mellan medlemsstaterna och vars sekretariat förvaltas av kommissionen).

[32] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

[33] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)*, COM(2017) 477 final, 13.9.2017.

[34] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden*, COM(2018) 225 final, 17.4.2018.

[35] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets direktiv om fastställande av harmoniserade bestämmelser för utseende av rättsliga företrädare för insamling av bevisning i straffrättsliga förfaranden*. COM(2018) 226 final, 17.4.2018.

[36] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum,* COM(2018) 630 final, 12.9.2018.

[37] H. Carrapico och A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?* (EU som en konsekvent (cyber)säkerhetsaktör?), Journal of Common Market Studies, vol. 55, nr 6, 2017.

[38] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017.

[39] Europaparlamentets utredningstjänst, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects* (transatlantisk cyberosäkerhet och it-brottslighet; ekonomisk påverkan och framtidsutsikter), PE 603.948, december 2017.

[40] Enisa, *An evaluation framework for Cyber Security Strategies* (en utvärderingsram för strategier för cybersäkerhet), 27.11.2014.

[41] Ett undantag är artikel 14 (”Övervakning och statistik”) i Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF.

[42] Europeiska ekonomiska och sociala kommittén, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (cybersäkerhet: säkerställa medvetenhet och resiliens i den privata sektorn i Europa inför ökande cyberrisker), mars 2018. CEPS-ECRI-arbetsgruppen, *Cybersecurity in Finance: Getting the policy mix right!* (cybersäkerhet inom finans: hitta rätt policymix!), juni 2018.

[43] 24 av de 28 nationella revisionsorganen svarade på vår enkät.

[44] Detta innebär principbaserad och så teknikneutral som möjligt.

[45] Europeiska kommissionens mekanism för vetenskaplig rådgivning, vetenskapligt yttrande 2/2017, 24.3.2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (EU:s digitala autonomi: ett möjligt tillvägagångssätt), *Digma Zeitschrift für Datenrecht und Informationssicherheit*, september 2018. European Centre for Political Economy, ibid., occasional paper nr 2/18, februari 2018.

[47] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets direktiv om vissa aspekter på avtal om tillhandahållande av digitalt innehåll*, COM(2015) 634 final, 9.12.2015.

[48] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets direktiv om vissa aspekter på avtal om försäljning av varor på nätet och annan distansförsäljning av varor*, COM(2017) 635 final, 9.12.2015.

[49] Nederländska cybersäkerhetsrådet, *European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care*, (European Foresights cybersäkerhetsmöte 2016: offentlig-privata akademiska rekommendationer till Europeiska kommissionen om sakernas internet och harmonisering av aktsamhetskrav), 2016.

[50] Centre for European Policy Studies, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* (information om säkerhetsbrister i programvaror i Europa: teknik, politik och rättsliga utmaningar – rapport från en CEPS-arbetsgrupp), juni 2018.

[51] Europeiska kommissionen, *Maximalt utnyttjande av it-säkerhetsdirektivet – mot ett effektivt genomförande av direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen*, COM(2017) 476 final/2, 4.10.2017.

[52] Europol, ibid., 2017.

[53] Europeiska unionens råd, *Slutrapport om den sjunde omgången av ömsesidiga utvärderingar om det praktiska genomförandet och verkan av europeisk politik för förebyggande och bekämpning av it-brottslighet*, 12711/1/17 REV 1, 9.10.2017.

[54] Europeiska kommissionen, *Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment* (konsekvensbedömning som åtföljer dokumentet Förslag till direktiv om bekämpande av bedrägeri och förfalskning som rör andra betalningsmedel än kontanter), SWD/2017/0298 final, 13.9.2017. Politisk enighet om den nya lagstiftningen nåddes i december 2018 och den förväntas antas i början av 2019.

[55] Europol, ibid., 2017.

[56] C-362/14: Maximillian Schrems mot Data Protection Commissioner (Irland), 6.10.2015.

[57] Europol/Eurojust, *Common challenges in combating cybercrime* (vanliga utmaningar vid bekämpning av it-brottslighet), 7021/17, 13.3.2017.

[58] European Commission, *Assessment of the EU 2013 Cybersecurity Strategy* (bedömning av EU:s strategi för cybersäkerhet från 2013), SWD(2017) 295 final, 13.9.2017.

[59] Europaparlamentets utredningstjänst, *Briefing: EU Legislation in Progress – Review of dual-use export controls* (briefing: pågående EU-lagstiftning – översyn över exportkontroller av produkter med dubbla användningsområden), PE589.832.

[60] Europaparlamentets resolution, *Mänskliga rättigheter och teknik: effekterna för de mänskliga rättigheterna i tredjeländer av system för intrång och övervakning*, (2014/2232(INI)), 8.9.2015. Varor och tjänster med dubbla användningsområden, vilket inbegriper programvaror och teknik, kan ha civila och militära tillämpningar.

[61] Den offentligt tillgängliga informationen lagras i WHOIS-databasen som förvaltas av ICANN (Internet Corporation for Assigned Names and Numbers). ICANN förvaltar domännamnssystemet. Missbruk av domännamn underlättar it-brottslighet.

[62] Artikel 3 i NIS-direktivet, ibid.

[63] Atlantic Council, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (riskkoppling: överväldigad av cyberrisker? ekonomiska fördelar och kostnader för alternativa cyberframtider), 10.9.2015.

[64] Vita huset, *Cybersecurity spending fiscal year 2019* (utgifter för cybersäkerhet för räkenskapsåret 2019).

[65] Europeiska kommissionen, *arbetsdokument från kommissionens avdelningar: Impact Assessment Accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027* (konsekvensbedömning som åtföljer förslaget till Europaparlamentets och rådets förordning om inrättande av programmet för ett digitalt Europa för perioden 2021–2027), SWD(2018) 305 final, 6.6.2018.

[66] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective* (nederländska investeringar i IKT och cybersäkerhet: sätta det i perspektiv), december 2016.

[67] Europeiska kommissionen, ibid., COM(2018) 630 final, 12.9.2018.

[68] Europaparlamentets utredningstjänsts framsynsenhet, *Achieving a sovereign and trustworthy ICT industry in the EU* (uppnå en oberoende och tillförlitlig IKT-bransch i EU), december 2017.

[69] European Digital SME Alliance, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (ståndpunktsdokument om EU:s strategi för cybersäkerhet: främja ekosystemet för små och medelstora företag), 31.7.2017.

[70] Europaparlamentets utredningstjänsts framsynsenhet, ibid., december 2017.

[71] Ibid.

[72] Europeiska kommissionen, *Impact assessment on the proposed research competence centre and network of national coordination centres* (konsekvensbedömning av förslaget om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum), SWD(2018) 403 final (del 1/4), 12.9.2018.

[73] Europeiska kommissionen, ibid., COM(2018) 630 final, 12.9.2018.

[74] Revisionsrättens särskilda rapport nr 13/2018: *Bekämpning av radikalisering som leder till terrorism*.

[75] Siffrorna i det här avsnittet kommer från kommissionens offentligt tillgängliga handlingar, förutom uppgiften 42 miljoner euro i punkt ***51***, som vi fick direkt från kommissionen.

[76] Horisont 2020 är EU:s forsknings- och innovationsprogram med ett värde på 80 miljarder euro, som stöder innovationsunionen och som syftar till att säkerställa EU:s globala konkurrenskraft.

[77] Horisont 2020, samhällsutmaning 7 ”Säkra samhällen – att skydda EU:s och dess invånares frihet och säkerhet”.

[78] Vi analyserade H2020-projekt från CORDIS-datamängden. Vi utförde textvektorisering på respektive projekts beskrivning med hjälp av JRC:s taxonomi för cybersäkerhet (se ***ruta 5*** i nästa kapitel) i syfte att identifiera projekt som sannolikt var cybersäkerhetsrelaterade. Vi kontrollerade och analyserade sedan resultaten manuellt.

[79] Europeiska cybersäkerhetsorganisationen (Ecso), *ECS cPPP Progress Monitoring Report 2016-2017* (rapport om övervakningen av framstegen i det avtalsbaserade offentlig-privata partnerskapet för cybersäkerhet i EU), 29.10.2018.

[80] Artikel 9.2 i NIS-direktivet, ibid.

[81] GLACY+ (Global Action on Cybercrime+) är ett gemensamt projekt med Europarådet. Det stöder tolv länder i Afrika, Asien–Stillahavsområdet och Latinamerika och Karibien, som i sin tur utgör nav som kan dela med sig av sin erfarenhet i sina respektive regioner.

[82] Europeiska centrumet för politisk strategi (EPSC), kommissionens tankesmedja, har kommenterat risken för att en "digital död vinkel" uppstår om gapet mellan EU och dess grannar på västra Balkan fortsätter att öka. Länder såsom Kina och Ryssland investerar avsevärda summor i regionen, vilket marginaliserar EU som en cyberaktör i regionen. Källa: EPSC, *Engaging with the Western Balkans: an investment in Europe's security* (samarbete med västra Balkan: en investering i Europas säkerhet), 17.5.2018.

[83] Europeiska investeringsbanken, *The EIB Group Operating Framework and Operational Plan 2018* (EIB-gruppens verksamhetsram och verksamhetsplan 2018), 12.12.2017. Ingen ytterligare information fanns tillgänglig vid tiden för utarbetandet.

[84] Europeiska kommissionen, *Förslag till Europaparlamentets och rådets förordning om inrättande av programmet för ett digitalt Europa för perioden 2021–2027*, COM(2018) 434 final, 6.6.2018.

[85] Europeiska kommissionen, *Europaparlamentets och rådets förordning (EU) 2018/1092 av den 18 juli 2018 om inrättande av ett europeiskt försvarsindustriellt utvecklingsprogram som syftar till att stödja konkurrenskraften och innovationsförmågan inom unionens försvarsindustri* (EUT L 200, 7.8.2018, s. 30). Dessutom har en förberedande åtgärd för försvarsrelaterad forskning, på sammanlagt 90 miljoner euro för perioden 2017–2019 och finansierad av H2020, upprättats under 2017. Det är oklart om den inbegriper cyberrelaterade utgifter.

[86] Revisionsrätten planerar att offentliggöra ett separat briefingdokument om EU:s försvar under 2019.

[87] Europols EC3, Enisa, Europeiska utrikestjänsten, Europeiska försvarsbyrån och CERT-EU har en personalstyrka på 159 personer. Den här totalsumman omfattar inte cyberrelaterad personal vid Europeiska kommissionen eller i medlemsstaterna. Källa: Centre for European Policy Studies, ibid., november 2018.

[88] *Enisa-utvärdering*, 2017.

[89] Europol begärde en årlig personalökning på 70 tillfälligt anställda i sin fleråriga plan för 2018–2020, men endast en ökning på 26 stycken godkändes för 2018. I nästa utkast till flerårig plan för 2019–2021 väger Europol in en blygsam ökning och antar att en större efterfrågan på resurser inte skulle hörsammas. Källa: Samråd om utkast till fleråriga program 2019–2021, inlämnat till den gemensamma parlamentariska kontrollgruppen, A 000834, 1.2.2018.

[90] *Enisa-utvärdering*, 2017. Mellan 2014 och 2016 användes omkring 80 % av Enisas driftsbudget för att upphandla studier.

[91] Enisa, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (utforska möjligheterna och begränsningarna med aktuella plattformar för underrättelser om hot), december 2017.

[92] ISACA (kallades tidigare Information Systems Audit and Control Association), *Information Security Governance: Guidance for Boards of Directors and Executive Management* (styrning av informationssäkerhet: vägledning för styrelser och verkställande ledning), andra utgåvan, 2006.

[93] EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (återuppnådd cybersäkerhet: förberedelser för cyberangrepp. 20:e globala informationssäkerhetsenkäten 2017), s. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy och H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (succé eller myt? förstå cybersäkerhetsprogrammens verkliga kostnad och inverkan), juli 2017.

[95] Securities and Exchange Commission, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (uttalande och tolkningsriktlinje om offentligägda företags information om cybersäkerhet), 21.2.2018.

[96] Ett forum för samarbete mellan Europeiska bankmyndigheten, Europeiska värdepappers- och marknadsmyndigheten samt Europeiska försäkrings- och tjänstepensionsmyndigheten.

[97] Europeiska värdepappers- och marknadsmyndigheten, *Joint Committee report on risks and vulnerabilities in the EU financial system* (rapport från den gemensamma kommittén om risker och säkerhetsbrister i EU:s finanssystem), april 2018.

[98] Enisa, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (standarder för informationssäkerhet och integritet för små och medelstora företag: rekommendationer för att förbättra antagandet av standarder för informationssäkerhet och integritet på små och medelstora företag), december 2015.

[99] Avseende EU:s medlemsstater har kommissionens mekanism för vetenskaplig rådgivning noterat en avsevärd och unik samförståndsnivå kring grundläggande principer och värden samt ett delat strategiskt intresse som kan stå i centrum för ändamålsenlig EU-styrning av cybersäkerhet. Källa: Vetenskapligt yttrande 2/2017, 24.3.2017.

[100] Förenta staterna, Kina, Japan, Sydkorea, Indien och Brasilien.

[101] Europeiska säkerhets- och försvarsakademin (T. Renard och A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (handbok om cybersäkerhet, kapitel 3.4 EU som partner i cyberdiplomati och -försvar), 23.11.2018.

[102] Europeiska unionens råd, *Handlingsplan för genomförandet av rådets slutsatser om det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU*, 15748/17, 12.12.2017.

[103] Europeiska kommissionen, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission* (Europeiska kommissionens digitala strategi: en digitalt förändrad, användarfokuserad och datadriven kommission), C(2018) 7118 final, 21.11.2018.

[104] Kommissionsledamot Mariya Gabriels svar på den skriftliga parlamentsfrågan (E-004294-17), 28.6.2017.

[105] Europeiska unionens råd, *Annual Report on the Implementation of the Cyber Defence Policy Framework* (årsrapport om genomförandet av ramen för politiken för it-försvar), 15870/17, 19.12.2017.

[106] Beslut 2015/443, 2015/444 och 2017/46 reglerar säkerheten i kommissionens kommunikations- och informationssystem. Genom kommissionens beslut C(2018) 7706 av den 21 november 2018 upprättas en styrelse för informationsteknik och cybersäkerhet, vilket slår samman den tidigare it-styrelsen och styrelsen för informationssäkerhet.

[107] Europeiska ekonomiska och sociala kommittén, ibid., mars 2018.

[108] Europaparlamentet, ibid., september 2015.

[109] EU:s gemensamma enhet för hybridhot inrättades 2016 inom Europeiska utrikestjänstens underrättelse- och lägescentral. Den tar emot och analyserar sekretessbelagd information och information från öppna källor från olika aktörer angående hybridhot.

[110] Enisa, *National-level Risk Assessments: An Analysis Report* (riskbedömningar på nationell nivå: en analysrapport), november 2013.

[111] Europeiska kommissionen, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act* (konsekvensbedömning av EU:s cybersäkerhetsbyrå och cybersäkerhetsakt), SWD(2017) 500 final (del 1/6), 13.9.2017.

[112] Europeiska kommissionen, ibid., SWD(2018) 403 final, 12.9.2018.

[113] Résaux IP Européens Network Coordination Centre, Europas regionala internetregister, som övervakar tilldelningen och registreringen av IP-adresser.

[114] Enisa, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (EISAS storskaliga pilotprojekt för gemensam ökad medvetenhet för EU-medborgare och små och medelstora företag), november 2012.

[115] Centre for Cyber Safety and Education, tillsammans med Booz Allen Hamilton, Alta Associates och Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (2017 års studie av den globala arbetskraften inom informationssäkerhet – måttstockar för arbetskraftens kompetens och hantering av cyberrisker).

[116] Europeiska ekonomiska och sociala kommittén, ibid., mars 2018.

[117] ,House of Lords House of Commons Joint Committee on the National Security Strategy *Cyber Security Skills and the UK's Critical National Infrastructure, Second Report of Session 2017–19* (cybersäkerhetskompetens och Förenade kungarikets kritiska nationella infrastruktur, andra rapporten för sessionen 2017–2019), 16.7.2018.

[118] Europol/Eurojust, *Common challenges in combating cybercrime* (vanliga utmaningar vid bekämpning av it-brottslighet), 7021/17, 13.3.2017.

[119] Europol/Eurojust, ibid., 7021/17, 13.3.2017.

[120] Europeiska kommissionen, ibid., SWD(2018) 403 final, 12.9.2018.

[121] Cepol, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (styrelsens beslut 33/2018/MB om Cepols samlade programdokument 2020–2022), 20.11.2018.

[122] Till exempel samarbete mellan Europeiska utrikestjänsten, medlemsstaterna, byråer och organ som Cepol, ECTEG eller Esfa.

[123] Enisa, *Stock-taking of information security training needs in critical sectors* (inventering av behovet av utbildning inom informationssäkerhet i kritiska sektorer), december 2017.

[124] Europeiska utbildningsgruppen för it-brottslighet.

[125] Europeiska kommissionen, *Trettonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, COM(2018) 46 final, 24.1.2018.

[126] Baserat på observationer i särskild rapport nr 14/2018, ibid.

[127] Europaparlamentets resolution av den 13 juni 2018 om it-försvar (2018/2004(INI)). Europeiska unionens råd, ibid., 15870/17, 19.12.2017.

[128] Schweiz, f.d. jugoslaviska republiken Makedonien, Ukraina, Bosnien-Hercegovina, Kosovo (denna beteckning påverkar inte ståndpunkter om Kosovos status och är i överensstämmelse med FN:s säkerhetsråds resolution 1244/1999 och med Internationella domstolens utlåtande om Kosovos självständighetsförklaring), Turkiet och Förenta staterna.

[129] Europol, *Internet Organised Crime Threat Assessment 2018* (hotbildsbedömning avseende den organiserade brottsligheten 2018).

[130] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman och S. Furman, *Security Fatigue*, (säkerhetsutmattning), *IT Professional*, vol. 18, nr 5, 2016, s. 26–32. Se även NIST.

[132] Europeiska kommissionen/Europeiska utrikestjänsten, *Att öka motståndskraften och stärka Att öka motståndskraften och stärka kapaciteten att hantera hybridhot*, JOIN(2018) 16 final, 13.6.2018.*t*

[133] Till exempel nedstängningen av AlphaBay och Hansa i gemensamma insatser som leddes av FBI och Nederländernas nationella polis med stöd av Europol. Det här var två av de största marknadsplatserna för handel med olagliga varor som droger, vapen och verktyg för it-brottslighet, till exempel sabotageprogram. Källa: Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure* (brottslighet på darkweb: samordnad brottsbekämpning är det enda botemedlet), pressmeddelande, 29.5.2018.

[134] Europeiska kommissionen, ibid., SWD(2018) 403 final, 12.9.2018.

[135] Europeiska unionens råd, ibid., 12711/1/17 REV 1, 9.10.2017.

[136] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017.

[137] Europeiska kommissionen/Europeiska utrikestjänsten, ibid., JOIN(2018) 16, 13.6.2018.

[138] Europeiska kommissionen, SWD(2017) 500 final, 13.9.2017.

[139] *Samförståndsavtal – Enisa, EDA, Europol EC3 och CERT-EU*, 23.5.2018.

[140] Europeiska kommissionen, anbudsförfarande: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* (upprätta och driva ett pilotprojekt för ett kompetensnätverk för cybersäkerhet för att utveckla och genomföra en gemensam färdplan för forskning och innovation inom cybersäkerhet), 27.10.2017.

[141] Jean-Claude Juncker, Uppdragsbeskrivning för kommissionsledamoten för säkerhetsunionen, 2.8.2016. Försvar hör inte till arbetsgruppens ansvarsområde.

[142] Europeiska unionens råd, *EU cybersecurity roadmap* (EU:s färdplan för cybersäkerhet), 8901/17, 11.5.2017.

[143] Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues* (debattera säkerhet plus: crowdsourcing-lösningar på världens säkerhetsfrågor), 5:e utgåvan, november 2017.

[144] JRC:s tekniska rapporter, karta över europeiska cybersäkerhetsexpertcentrum: *Definitioner och taxonomi.* Impact Assessment on the proposed Research Competence Centre and the Network of National Coordination Centres (konsekvensbedömning av förslaget om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum), SWD(2018) 403 final, 12.9.2018.

[145] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017.

[146] Europeiska kommissionen, ibid., SWD(2018) 403 final, 12.9.2018.

[147] Till exempel inbegriper de europeiska finansinstitutens informations- och analyscentraler representanter från finanssektorn, nationella CERT, brottsbekämpande organ, Enisa, Europol, Europeiska centralbanken, Europeiska betalningsrådet och Europeiska kommissionen.

[148] Enisa, *Information Sharing and Analysis Centres (ISACs) Cooperative models* (samarbetsmodeller för informations- och analyscentraler), 14.2.2018.

[149] Europeiska unionens råd, ibid., 12711/1/17 REV 1, 9.10.2017.

[150] https://www.europol.europa.eu/empact.

[151] En studie som Accenture utförde 2018 i 15 länder fann att 87 % av de fokuserade cyberangreppen förhindrades: *2018 State of Cyber Resilience* (tillståndet för cyberresiliens 2018), 10.4.2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (cybersäkerhet tvingar fram en omprövning av strategisk autonomi), Oxford University Politics Blog, 14.9.2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (tre anledningar till att cyberhotsdetektering fortfarande är ineffektiv), *IT Pro*, 14.7.2017.

[154] Europeiska ekonomiska och sociala kommittén, *ibid.*, mars 2018.

[155] Europeiska kommissionen, *Åttonde rapporten om framsteg i riktning mot en effektiv och verklig säkerhetsunion*, COM(2017) 354 final, 29.6.2017.

[156] Se de olika publikationerna från NIS-samarbetsgruppen.

[157] PSD2: andra betaltjänstdirektivet, ECB/SSM: Europeiska centralbanken/gemensamma tillsynsmekanismen, Target 2: transeuropeiskt automatiserat expressöverföringssystem för realtidsbruttoavveckling (andra generationen), förordning nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Källa: CEPS-ECRI-arbetsgruppen, ibid., juni 2018.

[158] Europeiska kommissionen, *Rekommendation om samordnade insatser vid storskaliga cyberincidenter och cyberkriser*, C(2017) 6100 final, 13.9.2017.

[159] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017. Det finns flera mekanismer för krishantering, inbegripet mekanismen för integrerad politisk krishantering (IPCR), ARGUS (kommissionens krishanteringsmekanism), Europeiska utrikestjänstens krishanteringsmekanism, unionens civilskyddsmekanism och EU:s beredskapsprotokoll för brottsbekämpning.

[160] Dessutom kan detta leda till att artikel 42.7 i fördraget om Europeiska unionen (klausulen om ömsesidigt bistånd) eller artikel 222 i fördraget om Europeiska unionens funktionssätt (solidaritetsklausulen) åberopas.

[161] Europeiska kommissionen/Europeiska utrikestjänsten, ibid., JOIN(2018) 16, 13.6.2018. I december 2018 rapporterades påstådda hackningar av Europeiska utrikestjänstens diplomatiska kommunikationsnät, Coreu, i media (källa: *New York Times*, *Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (hackade europeiska kablar avslöjar en värld full av oro över Trump, Ryssland och Iran), 18.12.2018). Ärendet håller för närvarande på att utredas.

[162] Samarbetet kring tidiga varningar och ömsesidigt bistånd kräver också ytterligare utveckling: *Rådets slutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser*, 10085/18, 26.6.2018.

[163] Europaparlamentets utredningstjänst, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity actcybersecurity act* (briefing om pågående EU-lagstiftning: Enisa och en ny cybersäkerhetsakt), PE 614.643, september 2018.

[164] Europeiska ekonomiska och sociala kommittén, ibid., mars 2018.

[165] Europeiska unionens råd, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* (EU:s beredskapsprotokoll för brottsbekämpning (LE ERP) för stora gränsöverskridande cyberangrepp), 14893/18, december 2018.

[165] Snabbinsatsteam och ömsesidigt bistånd på området för cybersäkerhet, plattform för

utbyte av information om cyberhot och hantering av cyberincidenter. Källa: Europeiska

[166]Snabbinsatsteam och ömsesidigt bistånd på området för cybersäkerhet, plattform för

utbyte av information om cyberhot och hantering av cyberincidenter. Källa: Europeiska nionens råd, *Permanent strukturerat samarbete (Pesco) – uppdatering av projektförteckningen – översikt*, 19.11.2018.

[167] Europeiska unionens råd, *Slutsatser om en ram för en gemensam diplomatisk respons från EU mot skadlig it-verksamhet*, 9916/17, 7.6.2017.

[168] Europeiska unionens råd, *Rådets slutsatser om cyberdiplomati*, 6122/15, 11.2.2015.

[169] Europeiska unionens råd, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities* (utkast till riktlinjer för genomförande för ramen för en gemensam diplomatisk respons mot skadlig it-verksamhet), 13007/17.

[170] Att tillskriva ansvar för en incident förblir ett politiskt beslut som ska fattas av medlemsstaterna och inte alla av verktygslådans åtgärder kräver tillskrivning.

[171] Verktygslådan ledde inte till en gemensam åtgärd, utan enskilda medlemsstater antog Förenta staternas ståndpunkt.

[172] Europeiska unionens råd, *Slutsatser om skadlig it-verksamhet*, 7925/18, 16.4.2018.

[173] Datorsystem som används för att styra processer i olika industrier, till exempel allmännyttiga tjänster, kemisk och industriell tillverkning, livsmedelsbearbetning, transportsystem och -nav samt logistiktjänster.

[174] Enisa, ibid., december 2017.

[175] Till exempel offentlig förvaltning, kemiska industrier och kärnenergiindustrier, tillverkning, livsmedelsbearbetning, turism, logistik och civilskydd.

[176] Europeiska kommissionen, ibid., SWD(2017) 295 final, 13.9.2017.

[177] Anförande av kommissionsledamot Věra Jourová vid Europaparlamentets plenarsammanträde om att *öka EU:s motståndskraft mot påverkan från utländska aktörer på den kommande valkampanjen inför valet i Europaparlamentet*, 14.11.2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (rysk valinblandning: Europas motattack mot falska nyheter och cyberangrepp), 23.5.2018.

[179] European Political and Strategy Centre (L. Past), *Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses* (cybersäkerhet i valteknik: oundvikliga angrepp och olika typer av hantering), i: *Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts* (valinblandning i den digitala tidsåldern – skapa motståndskraft mot it-baserade hot: en samling av artiklar från 35 ledande yrkesverksamma och experter), 2018.

[180] Enligt rådets direktiv 2008/114/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet av att stärka skyddet av denna.

[181] Europeiska kommissionens rekommendation om nätverk för valsamarbete, insyn på nätet, skydd mot cyberincidenter och bekämpning av desinformationskampanjer i samband med val till Europaparlamentet, C(2018) 5949 final, 12.9.2018.

[182] Europeiska rådets slutsatser, EUCO 11/15, 20.3.2015. Två ytterligare arbetsgrupper har tillkommit sedan dess, en för västra Balkan och en för södra grannskapet.

[183] En rapport från Atlantic Council uppmanade EU att begära att alla medlemsstater skickar nationella experter till arbetsgruppen. Se: D. Fried och A. Polyakova, *Democratic Defense Against Disinformation* (demokratiskt försvar mot desinformation), 5.3.2018.

[184] Ursprungligen saknade arbetsgruppen en egen budget, men 2018 tilldelades den 1,1 miljoner euro från Europaparlamentet för en förberedande ”StratCom Plus”-åtgärd.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), ibid., 23.5.2018.

[186] Europeiska kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik, *Åtgärdsplan mot desinformation*, JOIN(2018) 36 final. Planen fokuserar på att förbättra EU-institutionernas kapacitet att upptäcka, analysera och avslöja desinformation, stärka samordnad och gemensam hantering, mobilisera den privata sektorn, öka medvetenheten och förbättra samhällets motståndskraft.

[187] Europeiska kommissionen, *Bekämpande av desinformation online: en EU-strategi*, COM(2018) 236 final, 26.4.2018.

[188] Bör inte förväxlas med uppförandekoden om motverkande av olaglig hatpropaganda över internet.

[189] JRC, *The digital transformation of news media and the rise of disinformation and fake news* (nyhetsmediernas digitala omvandling och ökningen av desinformation och falska nyheter), JRC:s tekniska rapporter, JRC Digital Economy Working Paper 2018-02, april 2018.

[190] Enisa, *Strengthening Network & Information Security & Protecting Against Online Disinformation (“Fake News”)* (stärka nätverks- och informationssäkerhet samt skydda mot desinformation online (”falska nyheter”)), april 2018

[191] European Political and Strategy Centre (C. Frutos López), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (ett ansvar att stödja valorganisationer i att förutse och bekämpa cyberhot), i: ibid, 2018.

[192] Europeiska kommissionen, ibid., SWD(2018) 403 final, 12.9.2018.

[193] Förslaget till förordning (COM(2017) 487 final, 13.9.2018) om granskning av utländska direktinvesteringar, som lämnades in i september 2017, genomgår nu lagstiftningsförfarandet. I synnerhet omfattas kritisk teknik, som inbegriper artificiell intelligens, cybersäkerhet och applikationer med dubbla användningsområden.

[194] Europeiska kommissionen/Europeiska utrikestjänsten, ibid., JOIN(2017) 450 final, 13.9.2017.

Revisionsrättens team

Det här briefingdokumentet *Utmaningar för en ändamålsenlig EU-politik för cybersäkerhet* har antagits av avdelning III yttre åtgärder, säkerhet och rättvisa, där ledamoten Bettina Jakobsen är ordförande. Arbetet leddes av revisionsrättens ledamot Baudilio Tomé Muguruza med stöd av Daniel Costa de Magalhaes (kanslichef) och Ignacio Garcia de Parada (attaché), Alejandro Ballester-Gallardo (förstechef), Michiel Sweerts (uppgiftsansvarig), Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone och Silvia Monteiro Da Cunha (revisorer) och Johannes Bolkart (praktikant). Hannah Critoph gav språkligt stöd.

Från vänster till höger: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EUROPEISKA
REVISIONSRÄTTEN

Publikationsbyrån

EUROPEISKA REVISIONSRÄTTEN
12, rue Alcide De Gasperi
1615 Luxemburg
LUXEMBURG

Tfn +352 4398-1

Frågor: eca.europa.eu/sv/Pages/ContactForm.aspx
Webbplats: eca.europa.eu
Twitter: @EUAuditors

© Europeiska unionen, 2019
För all användning eller återgivning av foton eller annat material som Europeiska unionen inte har upphovsrätten till, exempelvis logotyperna i figur 4 samt bilagorna I och II, måste tillstånd inhämtas direkt från upphovsrättsinnehavaren.
Omslag: © Syda Productions / Shutterstock.com