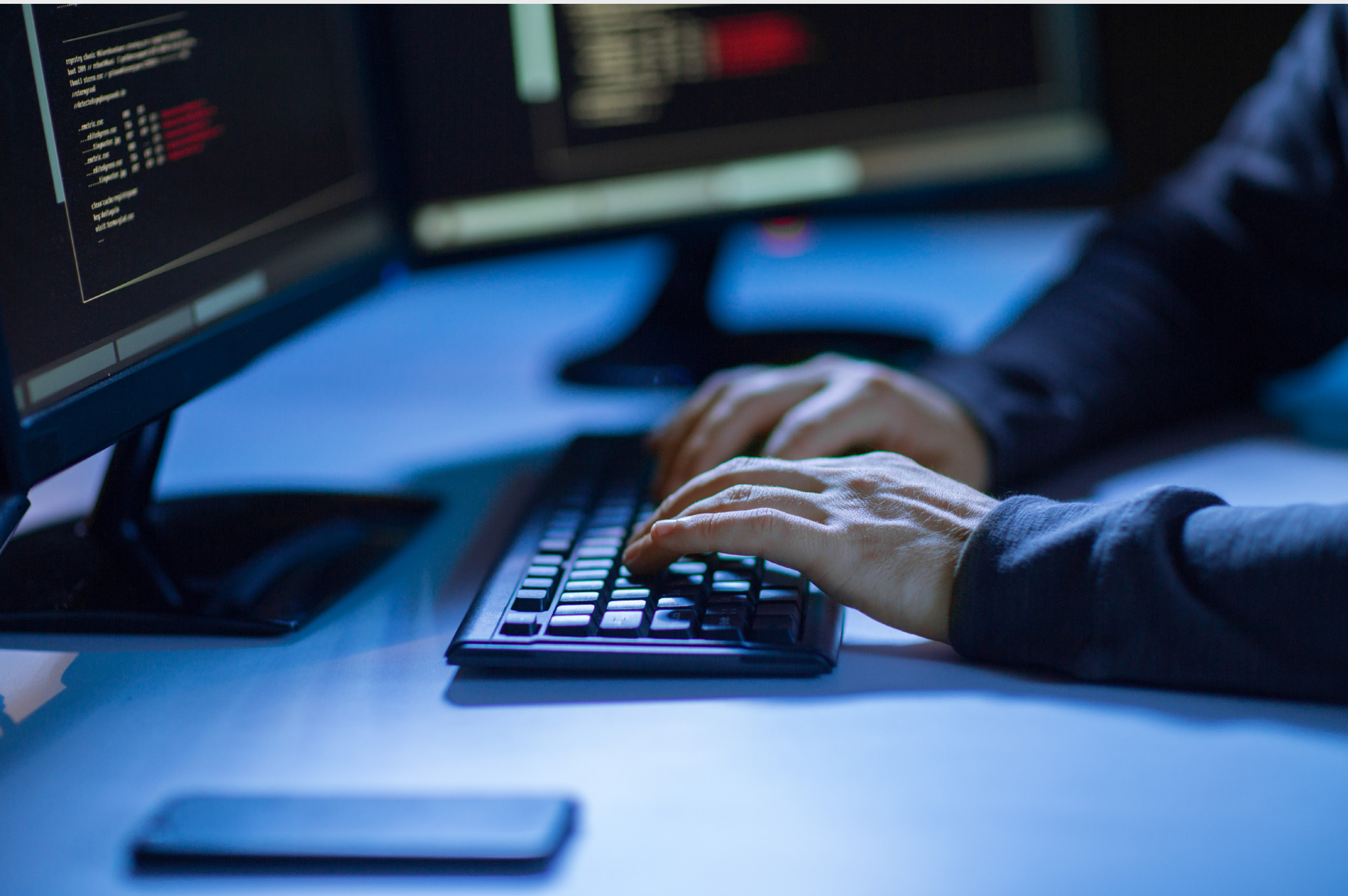
IL-QORTI EWROPEA TAL-AWDITURI

MT 2018

Sfidi għal politika effettiva tal-UE fil-qasam taċ-ċibersigurtà

Dokument Informattiv u Analitiku

Marzu 2019



Dwar id-dokument:

L-objettiv ta' dan id-dokument informattiv u analitiku, li mhuwiex rapport tal-awditjar, huwa li jipprovdi stampa ġenerali tax-xenarju kumpless tal-politika tal-UE fil-qasam taċ-ċibersigurtà, u li jidentifika l-isfidi prinċipali għat-twettiq ta' politika effettiva. Huwa jkopri s-sigurtà tan-netwerks u tal-informazzjoni, iċ-ċiberkriminalità, iċ-ċiberdifiża u d-diżinformazzjoni. Dan id-dokument se jagħti wkoll informazzjoni dwar kwalunkwe xogħol tal-awditjar li se jitwettaq fil-futur f'dan il-qasam.

Aħna bbażajna l-analiżi tagħna fuq analiżi dokumentarja ta' informazzjoni disponibbli għall-pubbliku f'dokumenti uffiċjali, dokumenti ta' pożizzjoni u studji mwettqa minn partijiet terzi. Aħna wettaqna x-xogħol fuq il-post bejn April u Settembru 2018, u jittieħdu inkunsiderazzjoni l-iżviluppi li saru sa Diċembru 2018. Aħna kkomplementajna x-xogħol tagħna bi stħarriġ li ntbagħat lill-uffiċċji nazzjonali tal-awditjar fl-Istati Membri, u permezz ta' intervisti mal-partijiet ikkonċernati ewlenin mill-istituzzjonijiet tal-UE u ma' rappreżentanti mis-settur privat.

L-isfidi li identifikajna huma miġbura flimkien f'erba' raggruppamenti ġenerali: i) il-qafas ta' politika; ii) il-finanzjament u l-infiq; iii) il-bini tar-reżiljenza ċibernetika; iv) ir-rispons effettiv għal inċidenti ċibernetiċi. L-ilħuq ta' livell ogħla ta' ċibersigurtà fl-UE jibqa' test imperattiv. Għalhekk, aħna ntemmu kull kapitolu b'sensiela ta' ideat għal aktar riflessjoni minn dawk li jfasslu l-politika, mil-leġiżlaturi u mill-professjonisti.

Nixtiequ nirrikonoxxu l-feedback kostruttiv riċevut mis-servizzi tal-Kummissjoni, mis-Servizz Ewropew għall-Azzjoni Esterna, mill-Kunsill tal-Unjoni Ewropea, mill-ENISA, mill-Europol, mill-Organizzazzjoni Ewropea taċ-Ċibersigurtà, u mill-uffiċċji nazzjonali tal-awditjar fl-Istati Membri.

Werrej

	Paragrafu
Sommarju eżekuttiv	I-XIII
Introduzzjoni	01-24
X'inhi ċibersigurtà?	02-06
Kemm hija gravi l-problema?	07-10
L-azzjoni tal-UE dwar iċ-ċibersigurtà	11-24
Politika	13-18
Leġiżlazzjoni	19-24
Kostruzzjoni ta' qafas ta' politika u leġiżlattiv	25-39
Sfida 1: evalwazzjoni u obbligu ta' rendikont siewja	26-32
Sfida 2: indirizzar tal-lakuni fid-dritt tal-UE u t-traspożizzjoni mhux uniformi tiegħu	33-39
Finanzjament u nfiq	40-64
Sfida 3: allinjament tal-livelli ta' investiment mal-għanijiet	41-46
Żieda tal-investiment	41-44
Żieda tal-impatt	45-46
Sfida 4: stampa ġenerali ċara tal-infiq tal-baġit tal-UE	47-60
Infiq fuq iċ-ċibersigurtà li huwa identifikabbli	50-56
Infiq ieħor fuq iċ-ċibersigurtà	57-58
Inħarsu 'l quddiem	59-60
Sfida 5: forniment ta' riżorsi adegwati għall-aġenziji tal-UE	61-64
Bini ta' soċjetà reżiljenti għaċ-ċibernetika	65-100
Sfida 6: tisħiħ tal-governanza u l-istandards	66-81
Governanza tas-sigurtà tal-informazzjoni	66-75
Valutazzjonijiet tar-riskji u tat-theddid	76-78
Inċentivi	79-81

Sfida 7: żieda tal-ħiliet u s-sensibilizzazzjoni 82-90

Taħriġ, ħiliet u żvilupp tal-kapaċitajiet 84-87

Sensibilizzazzjoni 88-90

Sfida 8: skambju ta' informazzjoni u koordinazzjoni aħjar 91-100

Koordinazzjoni fost l-istituzzjonijiet tal-UE u mal-Istati Membri 92-96

Kooperazzjoni u skambju ta' informazzjoni mas-settur privat 97-100

Rispons effettiv għal inċidenti ċibernetiċi 101-117

Sfida 9: identifikazzjoni u rispons effettivi 102-111

Identifikazzjoni u notifika 102-105

Rispons ikkoordinat 106-111

Sfida 10: protezzjoni tal-infrastruttura kritika u l-funzjonijiet tas-soċjetà 112-117

Protezzjoni tal-infrastruttura 112-115

Tisħiħ tal-awtonomija 116-117

Kummenti finali 118-121

Anness I — Xenarju kumpless u b'diversi livelli li jinkludi ħafna atturi

Anness II — Infiq tal-UE fuq iċ-ċibersigurtà mill-2014 'il hawn

Anness III — Rapporti mill-uffiċċji tal-awditjar tal-Istati Membri tal-UE

Akronimi u abbrevjazzjonijiet

Glossarju

Tim tal-QEA

Sommarju eżekuttiv

I Bis-saħħa tat-teknoloġija, li l-prodotti u s-servizzi l-ġodda tagħha qed isiru parti integrali mill-ħajja tagħna ta’ kuljum, qed tinfetaħ dinja ġdida sħiħa ta’ opportunitajiet. Min-naħa l-oħra, qed jiżdied ir-riskju li wieħed jisfa vittma taċ-ċiberkriminalità jew ta’ ċiberattakk, li l-impatt tas-soċjetà u ekonomiku tiegħu qed ikompli jikber. Il-motivazzjoni reċenti tal-UE, mill-2017 'il hawn, biex taċċellera l-isforzi sabiex isaħħaħ iċ-ċibersigurtà u l-awtonomija diġitali tagħha ġiet għalhekk fi żmien kritiku.

II Dan id-dokument informattiv u analitiku, li mhuwiex rapport tal-awditjar u huwa bbażat fuq informazzjoni disponibbli għall-pubbliku, għandu l-għan li jipprovdi stampa ġenerali ta’ xenarju ta’ politika kumpless u mhux uniformi, kif ukoll li jidentifika l-isfidi prinċipali għall-implimentazzjoni ta’ politika effettiva. L-ambitu tad-dokument tagħna jkopri l-politika tal-UE fil-qasam taċ-ċibersigurtà, kif ukoll iċ-ċiberkriminalità u ċ-ċiberdifiża, u jinkludi wkoll l-isforzi għall-ġlieda kontra d-diżinformazzjoni. L-isfidi li identifikajna huma miġbura flimkien f’erba’ raggruppamenti ġenerali: i) il-qafas ta’ politika u leġiżlattiv; ii) il-finanzjament u l-infiq; iii) il-bini tar-reżiljenza ċibernetika; u iv) ir-rispons effettiv għal inċidenti ċibernetiċi. Kull kapitolu jinkludi xi punti ta’ riflessjoni dwar l-isfidi ppreżentati.

Il-qafas ta’ politika u leġiżlattiv

III L-iżvilupp ta’ azzjoni allinjata mal-għanijiet ġenerali tal-istrateġija tal-UE għaċ-ċibersigurtà li ssir l-ambjent diġitali l-aktar sikur fid-dinja mhuwiex faċli fin-nuqqas ta’ objettivi li jistgħu jitkejlu u ta’ biżżejjed *data* affidabbli. L-eżiti rarament jitkejlu u huma ftit l-oqsma ta' politika li ġew evalwati. Għalhekk, sfida ewlenija hija l-**iżgurar ta’ obbligu ta’ rendikont u ta’ evalwazzjoni siewja** permezz ta’ bidla lejn kultura tal-prestazzjoni li tinkorpora prattiki ta’ evalwazzjoni.

IV Il-qafas leġiżlattiv jibqa’ inkomplet. Il-**lakuni fid-dritt tal-UE u t-traspożizzjoni inkonsistenti tiegħu** jistgħu jagħmluha diffiċli għal-leġiżlazzjoni biex tilħaq il-potenzjal sħiħ tagħha.

Finanzjament u nfiq

V L-**allinjament tal-livelli ta’ investiment mal-għanijiet** huwa diffikultuż: dan jirrikjedi żieda mhux biss tal-investiment kumplessiv fil-qasam taċ-ċibersigurtà – li fl-UE kien baxx u frammentat– iżda wkoll żieda tal-impatt, speċjalment fl-isfruttar aħjar tar-

riżultati tal-infiq fuq ir-riċerka u l-iżgurar tal-immirar u l-finanzjment effettiv ta’ negozji li jkunu għadhom kemm jiftħu.

VI **Stampa ġenerali ċara tal-infiq tal-UE** hija essenzjali biex l-UE u l-Istati Membri tagħha jkunu jafu liema lakuni għandhom jimlew biex jissodisfaw l-għanijiet iddikjarati tagħhom. Billi ma hemmx baġit iddedikat tal-UE biex jiffinanzja l-istrateġija għaċ-ċibersigurtà, ma hemmx stampa ċara tal-fondi investiti u tal-iskop tagħhom.

VII Fi żmien ta’ prijoritajiet politiċi akbar xprunati mis-sigurtà, **limitazzjonijiet fil-forniment ta’ riżorsi adegwati tal-aġenziji rilevanti għaċ-ċiberspazju tal-UE** jistgħu jipprevienu l-ambizzjonijiet tal-UE milli jiġu mqabbla. L-indirizzar ta’ din l-isfida jinkludi s-sejba ta’ modi kif it-talent jiġi attirat u jinżamm.

Bini tar-reżiljenza ċibernetika

VIII Hemm għadd kbir ta’ dgħufijiet fil-governanza taċ-ċibersigurtà fis-settur pubbliku u dak privat fl-UE kif ukoll fil-livell internazzjonali. Dan ixekkel l-abbiltà tal-komunità globali li tirreaġixxi għal ċiberattakki u li tillimitahom, kif ukoll idgħajjef approċċ koerenti fil-livell tal-UE. L-isfida hija għaldaqstant li **tissaħħaħ il-governanza taċ-ċibersigurtà**.

IX Minħabba n-nuqqas globali dejjem akbar ta’ ħiliet fil-qasam taċ-ċibersigurtà, **iż-żieda tal-ħiliet u s-sensibilizzazzjoni** fis-setturi u l-livelli kollha tas-soċjetà huma essenzjali. Attwalment, hemm standards limitati fil-livell tal-UE għat-taħriġ, iċ-ċertifikazzjoni jew il-valutazzjonijiet tar-riskji ċibernetiċi.

X Pedament ta’ fiduċja huwa essenzjali għat-tisħiħ tar-reżiljenza ċibernetika kumplessiva. Il-Kummissjoni nfisha vvalutat li l-koordinazzjoni inġenerali għadha insuffiċjenti. It-**titjib fl-iskambju ta’ informazzjoni u l-koordinazzjoni** bejn is-settur pubbliku u dak privat jibqa’ sfida.

Rispons effettiv għal inċidenti ċibernetiċi

XI Is-sistemi diġitali saru tant kumplessi li huwa impossibbli jiġu pprevenuti l-attakki kollha. Ir-rispons għal din l-isfida huwa **identifikazzjoni u rispons rapidi**. Madankollu, iċ-ċibersigurtà għadha mhix integrata għalkollox fil-mekkaniżmi ta' koordinazzjoni eżistenti tar-rispons għall-kriżijiet fil-livell tal-UE, u dan potenzjalment jillimita l-kapaċità tal-UE li tirreaġixxi għal inċidenti ċibernetiċi transkonfinali fuq skala kbira.

XII Il-**protezzjoni tal-infrastruttura kritika u l-funzjonijiet tas-soċjetà** hija essenzjali. L-interferenza potenzjali fil-proċessi elettorali u l-kampanji ta' diżinformazzjoni huma sfida kruċjali.

XIII L-isfidi attwali ppreżentati mit-theddid ċibernetiku li l-UE u l-ambjent globali ġenerali qed jiffaċċjaw, jirrikjedu impenn kontinwat u aderenza soda u kontinwa mal-valuri fundamentali tal-UE.

Introduzzjoni

01 Bis-saħħa tat-teknoloġija qed tinfetaħ dinja ġdida sħiħa ta' opportunitajiet. Hekk kif jitniedu prodotti u servizzi ġodda, dawn isiru parti integrali mill-ħajja tagħna ta' kuljum. Madankollu, kull żvilupp ġdid iżid id-dipendenza teknoloġika tagħna, u l-istess tagħmel l-importanza taċ-ċibersigurtà. Aktar ma nqiegħdu *data* personali online u aktar ma nsiru konnessi, aktar ma jkun probabbli li nisfaw vittmi ta' xi forma ta' ċiberkriminalità jew ta' ċiberattakk.

X'inhi ċibersigurtà?

02 Ma hemmx definizzjoni standard u li hija aċċettata universalment ta' ċibersigurtà[1]. B'mod ġenerali, din tikkostitwixxi s-salvagwardji u l-miżuri kollha adottati biex jiddefendu s-sistemi ta' informazzjoni u lill-utenti tagħhom kontra aċċess mhux awtorizzat, attakk u ħsara biex jiġu żgurati l-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data*.

03 Iċ-ċibersigurtà tinvolvi l-prevenzjoni, l-identifikazzjoni, ir-rispons għal inċidenti ċibernetiċi u l-irkupru minnhom. L-inċidenti jistgħu jkunu intenzjonati jew le u jvarjaw, pereżempju, minn divulgazzjonijiet aċċidentali ta' informazzjoni, sa attakki fuq in-negozji u l-infrastruttura kritika, sas-serq ta' *data* personali, u anke interferenza fil-proċessi demokratiċi. Dawn kollha jista' jkollhom effetti estensivi li jagħmlu ħsara fuq l-individwi, l-organizzazzjonijiet u l-komunitajiet.

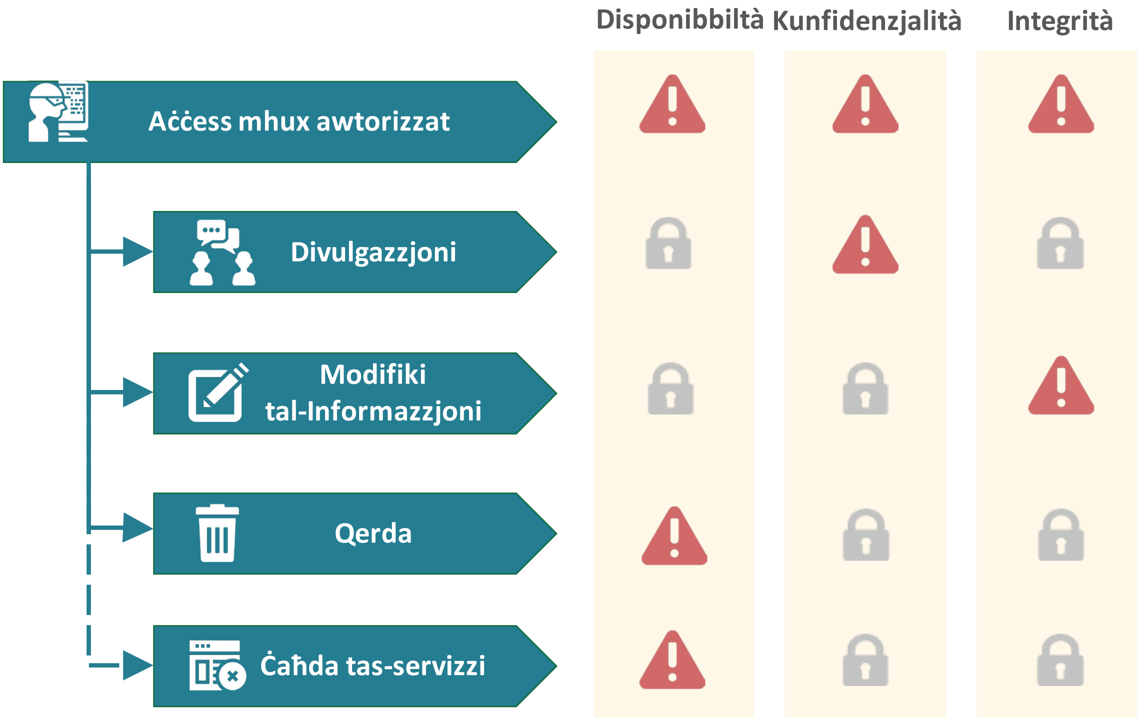
04 Bħala terminu użat fl-ambitu politiku tal-UE, iċ-ċibersigurtà mhijiex limitata għas-sigurtà tan-netwerks u tal-informazzjoni. Hija tkopri kwalunkwe attività illegali li tinvolvi l-użu ta' teknoloġiji diġitali fiċ-ċiberspazju. Għalhekk, din tista' tinkludi każijiet ta' ċiberkriminalità bħal tnedija ta' attakki minn virusijiet tal-kompjuter u frodi permezz ta' pagamenti mhux bi flus kontanti, kif ukoll tista' tnaqqas id-distakk bejn is-sistemi u l-kontenut, bħal bid-disseminazzjoni ta' materjal ta' abbuż sesswali tat-tfal online. Hija tista' tkopri wkoll kampanji ta' diżinformazzjoni biex jinfluwenzaw id-dibattitu online u interferenza elettorali suspettata. Barra minn hekk, l-Europol tqis li hemm konverġenza bejn iċ-ċiberkriminalità u t-terroriżmu[2].

05 Atturi differenti – inklużi Stati, gruppi kriminali u hackers – jinstigaw inċidenti ċibernetiċi, minħabba motivi differenti. Il-konsegwenzi ta' dawn l-inċidenti jinħassu fil-livell nazzjonali, f'dak Ewropew u anke f'dak globali. Madankollu, in-natura intanġibbli u fil-biċċa mingħajr konfini tal-internet, kif ukoll l-għodod u t-tattiki użati, spiss

jagħmluha diffiċli biex jiġi identifikat l-awtur ta' attakk (l-hekk imsejħa "problema tal-attribuzzjoni").

06 Il-bosta tipi ta' theddid ċibernetiku jista' jiġi kklassifikat skont l-effetti tagħhom fuq id-*data* – divulgazzjoni, modifiki, qerda, jew aċċess irrifjutat – jew il-prinċipji fundamentali ta' sigurtà tal-informazzjoni li jiksru, kif jidher fil-***Figura 1*** hawn taħt. Xi eżempji ta' attakki huma deskritti fil-***Kaxxa 1***. Hekk kif il-livell ta' sofistikazzjoni tal-attakki għas-sistemi ta' informazzjoni jiżdied, il-mekkaniżmi ta' difiża tagħna jsiru inqas effettivi[3].

Figura 1 – Tipi ta' theddid u l-prinċipji ta' sigurtà li huma jqiegħdu f'riskju



Sors: Il-QEA, immodifikat minn studju mwettaq mill-Parlament Ewropew[4]. Katnazz = l-ebda impatt fuq is-sigurtà; Punt esklamattiv = is-sigurtà tinsab f'riskju

Kaxxa 1

Tipi ta’ ċiberattakki

Kull darba li apparat ġdid jiġi online jew jiġi konness ma’ apparat ieħor, l-hekk imsejħa “superfiċje vulnerabbli għall-attakk” fil-qasam taċ-ċibersigurtà tiżdied. It-tkabbir esponenzjali tal-Internet tal-Oġġetti, il-cloud, il-big *data* u d-diġitalizzazzjoni tal-industrija huwa akkumpanjat minn żieda fl-esponiment ta’ vulnerabbiltajiet, li jippermetti lil atturi malizzjużi jimmiraw dejjem aktar vittmi. Id-diversi tipi ta’ attakki u l-livell dejjem jikber ta’ sofistikazzjoni tagħhom jagħmluha ġenwinament diffiċli li jinżamm il-pass[5].

Malware (software malizzjuż) huwa mfassal biex jagħmel ħsara lil apparat jew lil netwerks. Jista’ jinkludi virusijiet, trojans, software ta' riskatt, worms, adware u spyware. **Software ta' riskatt** jikkripta *data*, filwaqt li jipprevieni lill-utenti milli jkollhom aċċess għall-fajls tagħhom sakemm jitħallas riskatt, tipikament fi kriptovaluta, jew titwettaq azzjoni. Skont l-Europol, l-attakki minn software ta' riskatt jiddominaw fil-kategoriji kollha, u l-għadd ta’ tipi ta’ software ta' riskatt żdied sew matul l-aħħar ftit snin. Attakki **Distribwiti li Jwaqqfu s-Servizz** (DDoS), li permezz tagħhom is-servizzi jew ir-riżorsi ma jkunux disponibbli billi jintbagħtulhom aktar talbiet milli jifilħu, qed jiżdiedu wkoll, b’terz tal-organizzazzjonijiet li ffaċċjaw dan it-tip ta’ attakk fl-2017[6].

L-utenti jistgħu jiġu manipulati biex, inkonxjament, iwettqu azzjoni jew jiddivulgaw informazzjoni kunfidenzjali. Din l-astuzja tista’ tintuża għas-serq ta’ *data* jew għaċ-ċiberspjunaġġ, u hija magħrufa bħala **social engineering**. Hemm modi differenti biex dan jinkiseb, iżda metodu komuni huwa l-**phishing**, fejn posta elettronika li tkun tidher li ġejja minn sorsi fdati tqarraq bl-utenti biex jiżvelaw informazzjoni jew jikklikkjaw fuq links li jinfettaw l-apparat b’malware imniżżel. Aktar minn nofs l-Istati Membri rrappurtaw investigazzjonijiet relatati ma’ attakki fuq netwerks[7].

X’aktarx, it-tipi ta’ theddid l-aktar kiefra huma t-**theddid persistenti avvanzat** (APTs). Dawn jinkludu aggressuri sofistikati involuti f’monitoraġġ fuq terminu twil u f’serq ta’ *data*, u xi drabi jkunu wkoll qed jaħbu għanijiet qerrieda. L-għan tagħhom huwa li jibqgħu moħbija mingħajr ma jiġu identifikati għal kemm jista' jkun fit-tul. L-APTs huma spiss marbuta mal-Istat u jimmiraw lejn setturi partikolarment sensittivi bħat-teknoloġija, id-difiża u l-infrastruttura kritika. Iċ-ċiberspjunaġġ jitqies li jirrappreżenta mill-inqas kwart tal-inċidenti ċibernetiċi kollha u l-maġġoranza tal-ispejjeż[8].

Kemm hija gravi l-problema?

07 Minħabba n-nuqqas ta’ *data* affidabbli, huwa diffiċli li jinqabad l-impatt ta’ tħejjija ħażina għal ċiberattakk. L-impatt ekonomiku taċ-ċiberkriminalità żdied b’ħames darbiet bejn l-2013 u l-2017[9], u laqat lil gvernijiet u lil kumpaniji, kemm kbar kif ukoll

żgħar. It-tkabbir previst fil-primjums tal-assigurazzjoni ċibernetika minn EUR 3 biljun fl-2018 għal EUR 8.9 biljun fl-2020 jirrifletti din ix-xejra.

08 Filwaqt li l-impatt finanzjarju taċ-ċiberattakki qed ikompli jikber, hemm disparità allarmanti bejn l-ispiża tat-tnedija ta’ attakk u l-ispiża tal-prevenzjoni, l-investigazzjoni u l-kumpens. Pereżempju, attakk DDoS jista’ jiswa biss EUR 15 fix-xahar biex jitwettaq, madankollu, it-telf imġarrab min-negozju mmirat, inklużi d-danni għar-reputazzjoni, huwa konsiderevolment ogħla[10].

09 Għalkemm 80 % tan-negozji fl-UE esperjenzaw mill-inqas inċident wieħed taċ-ċibersigurtà fl-2016[11], ir-riskji f’dan ir-rigward għadhom qed jiġu injorati b’mod allarmanti. Fost il-kumpaniji fl-UE, 69 % ma għandhomx, jew għandhom biss fehim bażiku, tal-esponiment tagħhom għal theddid ċibernetiku[12], u 60 % qatt ma stamw it-telf finanzjarju potenzjali[13]. Barra dan, skont stħarriġ globali, terz tal-organizzazzjonijiet jippreferu jħallsu r-riskatt tal-hacker milli jinvestu fis-sigurtà tal-informazzjoni[14].

10 L-attakki globali mis-software ta' riskatt *Wannacry* u mill-malware li jħassar id-*data NotPetya*, li seħħew fl-2017, flimkien affettwaw aktar minn 320 000 vittma f’madwar 150 pajjiż[15]. Dawn l-inċidenti wasslu biex id-dinja kollha ssir taf dwar it-theddida li kienet qed tiġi ppreżentata minn ċiberattakki, u dan ħoloq momentum ġdid biex iċ-ċibersigurtà tkun parti mill-ħsieb politiku ġenerali. Barra minn hekk, 86 % taċ-ċittadini tal-UE issa jemmnu li r-riskju li wieħed jisfa vittma taċ-ċiberkriminalità qed jiżdied[16].

L-azzjoni tal-UE dwar iċ-ċibersigurtà

11 Fl-2001[17], l-UE saret organizzazzjoni osservatriċi għall-Kumitat tal-Konvenzjoni dwar iċ-Ċiberkriminalità tal-Kunsill tal-Ewropa (il-Konvenzjoni ta' Budapest). Minn dak iż-żmien 'il hawn, l-UE użat il-politika, il-leġiżlazzjoni u l-infiq biex ittejjeb ir-reżiljenza ċibernetika tagħha. Fi sfond ta’ għadd dejjem akbar ta’ ċiberattakki u inċidenti kbar, l-attività aċċellerat mill-2013 'il hawn, kif turi l-***Figura 2***. B’mod parallel, l-Istati Membri adottaw (u f’xi każijiet diġà aġġornaw) l-ewwel strateġiji nazzjonali għaċ-ċibersigurtà tagħhom.

12 L-atturi prinċipali tal-UE li huma responsabbli għaċ-ċibersigurtà huma deskritti fil-***Kaxxa 2*** u fl-***Anness I***.

Kaxxa 2

Min huwa involut?

Il-**Kummissjoni Ewropea** għandha l-għan li żżid il-kapaċitajiet u l-kooperazzjoni fil-qasam taċ-ċibersigurtà, issaħħaħ l-UE bħala attur taċ-ċibersigurtà, u tintegraha f'politiki oħra tal-UE. Id-Direttorati Ġenerali (DĠ) prinċipali responsabbli għall-politika fil-qasam taċ-ċibersigurtà huma d-DĠ **CNECT** (ċibersigurtà) u d-DĠ **HOME** (ċiberkriminalità), li huma responsabbli għas-Suq Uniku Diġitali u l-Unjoni tas-Sigurtà rispettivament. Id-DĠ **DIGIT** huwa responsabbli għas-sigurtà tal-IT tas-sistemi proprji tal-Kummissjoni.

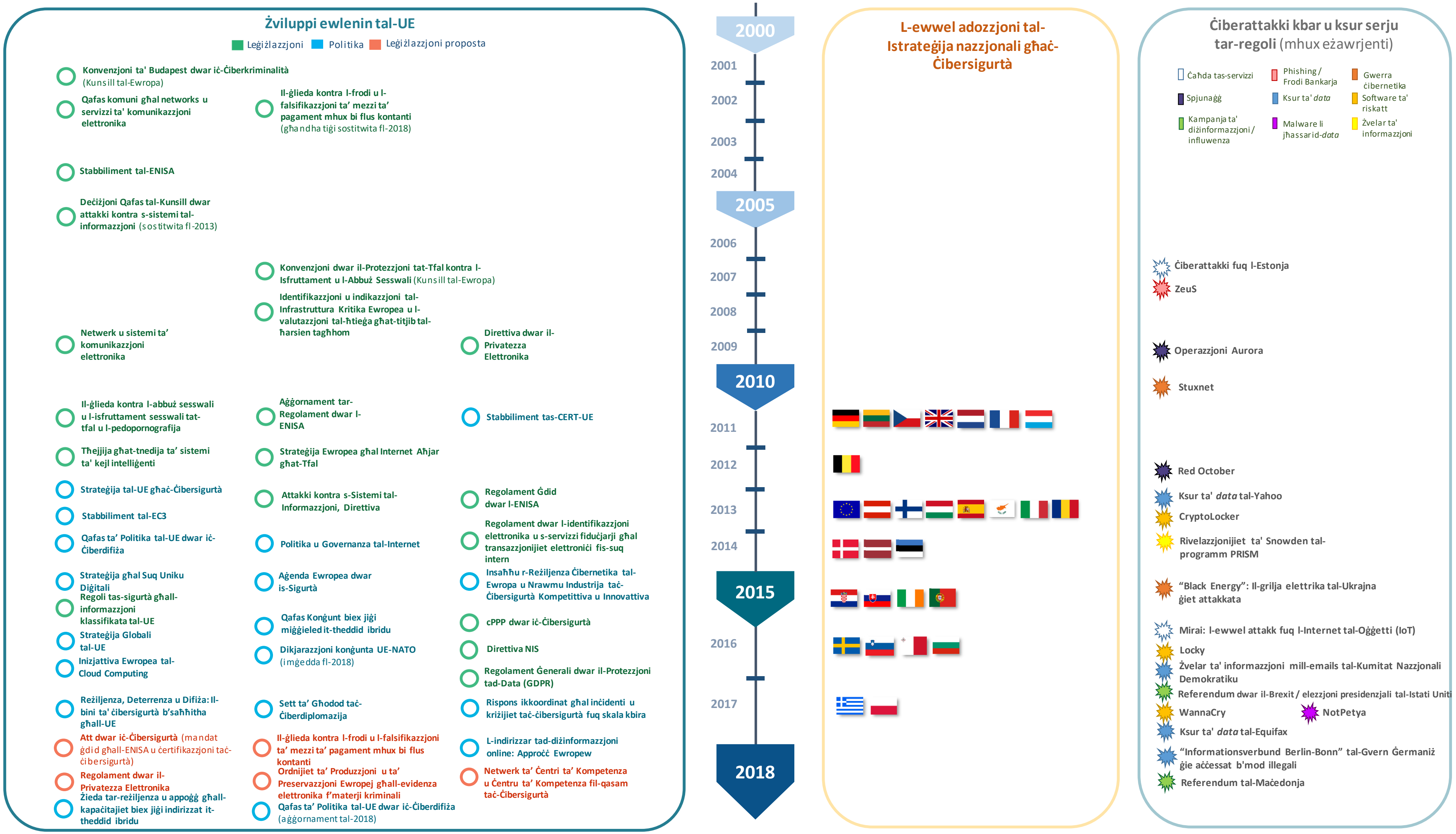
Ospitant tal-aġenziji tal-UE jappoġġa lill-Kummissjoni, notevolment l-**ENISA** (Aġenzija tal-Unjoni Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni), l-aġenzija tal-UE għaċ-ċibersigurtà – prinċipalment korp konsultattiv li jappoġġa l-iżvilupp tal-politika, it-tisħiħ tal-kapaċitajiet u ż-żieda tas-sensibilizzazzjoni. Iċ-Ċentru Ewropew taċ-Ċiberkriminalità tal-Europol (**EC3**) ġie stabbilit biex isaħħaħ ir-rispons mill-awtoritajiet tal-infurzar tal-liġi tal-UE għaċ-ċiberkriminalità. Skwadra ta' Rispons f'Emerġenza relatata mal-Kompjuters (**CERT-UE**), li tappoġġa lill-istituzzjonijiet, lill-korpi u lill-aġenziji kollha tal-Unjoni, hija ospitata mill-Kummissjoni.

Is-**Servizz Ewropew għall-Azzjoni Esterna** (SEAE) għandu rwol prinċipali fiċ-ċiberdifiża, fiċ-ċiberdiplomazija u fil-komunikazzjoni strateġika, u jospita ċentri tal-intelligence u tal-analiżi. L-**Aġenzija Ewropea għad-Difiża** (EDA) għandha l-għan li tiżviluppa kapaċitajiet għaċ-ċiberdifiża.

L-**Istati Membri** huma primarjament responsabbli għaċ-ċibersigurtà proprja tagħhom u, fil-livell tal-UE, jaġixxu permezz tal-**Kunsill**, li għandu bosta korpi ta' koordinazzjoni u ta' kondiviżjoni tal-informazzjoni (fosthom il-Grupp ta' Ħidma Orizzontali dwar Kwistjonijiet ta' Ċiberspazju). Il-**Parlament Ewropew** jaġixxi bħala koleġiżlatur.

L-**organizzazzjonijiet tas-settur privat**, inklużi l-industrija, il-korpi ta' governanza tal-Internet, u l-istituzzjonijiet akkademiċi, huma kemm sħab kif ukoll kontributuri għall-iżvilupp u l-implimentazzjoni tal-politika – inkluż permezz ta' sħubija pubblika-privata kuntrattwali (**cPPP**).

Figura 2 – Aċċellerazzjoni fl-iżvilupp tal-politika u fil-leġiżlazzjoni (fil-31 ta' Diċembru 2018)



Sors: Il-QEA.

Politika

13 L-ekosistema ċibernetika tal-UE hija kumplessa u għandha diversi livell, tkopri firxa wiesgħa ta’ oqsma ta' politika interna, bħal politiki dwar il-ġustizzja u l-affarijiet Interni, is-suq uniku diġitali u r-riċerka. Fil-qafas tal-politika esterna, iċ-ċibersigurtà hija karatteristika tad-diplomazija, u qed issir dejjem aktar parti mill-politika ta' difiża emerġenti tal-UE.

14 Il-pedament tal-politika tal-UE huwa l-**Istrateġija għaċ-Ċibersigurtà tal-2013**[18]. L-Istrateġija għandha l-għan li tagħmel l-ambjent diġitali tal-UE l-aktar wieħed sikur fid-dinja, filwaqt li tiddefendi l-valuri u l-libertajiet fundamentali. Hija għandha ħames objettivi fundamentali: (i) iżżid ir-reżiljenza ċibernetika; (ii) tnaqqas iċ-ċiberkriminalità; (iii) tiżviluppa politiki u kapaċitajiet għaċ-ċiberdifiża; (iv) tiżviluppa riżorsi industrijali u teknoloġiċi għaċ-ċibersigurtà; u (v) tistabbilixxi politika internazzjonali dwar iċ-ċiberspazju li tkun allinjata mal-valuri fundamentali tal-UE.

15 L-Istrateġija għaċ-Ċibersigurtà hija interkonnessa ma’ tliet srateġiji li ġew adottati sussegwentement:

— L-objettiv tal-**Aġenda Ewropea dwar is-Sigurtà** (2015) huwa li ttejjeb l-infurzar tal-liġi u r-rispons ġudizzjarju għaċ-ċiberkriminalità, prinċipalment billi jġġedded politiki u leġiżlazzjoni eżistenti li jkunu qed jiġu aġġornati[19]. Hija għandha wkoll l-għan li tidentifika ostakli għall-investigazzjonijiet kriminali dwar iċ-ċiberkriminalità u li ttejjeb it-tisħiħ tal-kapaċitajiet ċibernetiċi.

— L-**Istrateġija għal Suq Uniku Diġitali**[20] (2015) għandha l-għan li toħloq aċċess aħjar għall-prodotti u s-servizzi diġitali billi toħloq il-kundizzjonijiet it-tajbin li permezz tagħhom jiġi mmassimizzat il-potenzjal ta’ tkabbir tal-ekonomija diġitali. It-tisħiħ tas-sigurtà, il-fiduċja u l-inklużjoni online huwa essenzjali għal dan l-għan.

— L-**Istrateġija Globali**[21] tal-2016 għandha l-għan li tagħti spinta lir-rwol tal-UE fid-dinja. Iċ-ċibersigurtà tifforma pilastru fundamentali permezz ta’ impenn imġedded għal kwistjonijiet ta' ċiberspazju, kooperazzjoni ma’ sħab ewlenin, u riżoluzzjoni biex jiġu indirizzati kwistjonijiet ta' ċiberspazju fl-oqsma kollha ta’ politika, inkluża l-prova kontrarja ta’ diżinformazzjoni permezz ta’ komunikazzjoni strateġika.

16 Fi snin reċenti, billi ċ-ċiberspazju sar dejjem aktar militarizzat[22] u armat[23], beda jitqies bħala l-ħames dominju tal-gwerra[24]. Iċ-ċiberdifiża tipproteġi s-sistemi, in-networks u l-infrastruttura kritika taċ-ċiberspazju kontra attakki minn mezzi militari jew mezzi oħra. **Qafas ta’ Politika dwar iċ-Ċiberdifiża** ġie adottat fl-2014 u ġie aġġornat fl-

2018[25]. L-aġġornamenti tal-2018 jidentifikaw sitt prijoritajiet, inkluż l-iżvilupp ta’ kapaċitajiet għaċ-ċiberdifiża, kif ukoll il-protezzjoni tan-netwerks ta’ komunikazzjoni u ta’ informazzjoni tal-Politika ta’ Sigurtà u ta’ Difiża Komuni (PSDK) tal-UE. Iċ-ċiberdifiża tifforma wkoll parti mill-Qafas ta' Kooperazzjoni Strutturata Permanenti (PESCO) u mill-kooperazzjoni bejn l-UE u n-NATO.

17 Il-**Qafas Konġunt biex jiġi miġġieled it-theddid ibridu** tal-UE (2016) jindirizza theddid ċibernetiku kemm għall-infrastruttura kritika kif ukoll għall-utenti privati, filwaqt li jenfasizza li ċ-ċiberattakki jistgħu jitwettqu permezz ta’ kampanji ta' diżinformazzjoni fil-midja soċjali[26]. Huwa josserva wkoll il-ħtieġa li tittejjeb is-sensibilizzazzjoni u tissaħħaħ il-kooperazzjoni bejn l-UE u n-NATO, li ngħatat importanza fid-Dikjarazzjonijiet Konġunti UE-NATO tal-2016 u l-2018[27].

18 Fl-2017, il-Kummissjoni ppreżentat pakkett ġdid dwar iċ-ċibersigurtà, li kien jirrifletti l-urġenza dejjem akbar tal-protezzjoni diġitali. Dan kien jinkludi komunikazzjoni ġdida mill-Kummissjoni li taġġorna l-Istrateġija għaċ-Ċibersigurtà tal-2013[28], pjan ta’ azzjoni għal rispons veloċi u kkoordinat għal attakk kbir, u għall-implimentazzjoni rapida tad-Direttiva dwar is-Sigurtà tan-Netwerks u tas-Sistemi ta’ Informazzjoni (Direttiva NIS)[29]. Barra dan, il-pakkett kien jinkludi għadd ta’ proposti leġiżlattivi (ara l-paragrafu ***22***).

Leġiżlazzjoni

19 Mill-2002 ’il hawn, ġiet adotatta leġiżlazzjoni b’livelli differenti ta’ rilevanza għaċ-ċibersigurtà.

20 Bħala l-pilastru prinċipali tal-Istrateġija għaċ-Ċibersigurtà tal-2013, l-element ċentrali legali huwa d-**Direttiva dwar is-Sigurtà tan-Netwerks u tal-Informazzjoni (NIS)**[30] tal-2016, l-ewwel leġiżlazzjoni dwar iċ-ċibersigurtà għall-UE kollha. Id-direttiva, li kellha tiġi trasposta sa Mejju 2018, għandha l-għan li tikseb livell minimu ta’ kapaċitajiet armonizzati billi tobbliga lill-Istati Membri jadottaw strateġiji nazzjonali għan-NIS u joħolqu punti uniċi ta’ kuntatt u skwadri ta’ rispons għal inċidenti relatati mas-sigurtà tal-kompjuters (CSIRTs)[31]. Hija tistabbilixxi wkoll rekwiżiti ta' sigurtà u ta' notifika għal operaturi ta' servizzi essenzjali f’setturi kritiċi u għal fornituri ta' servizzi diġitali.

21 B’mod parallel, ir-**Regolament Ġenerali dwar il-Protezzjoni tad-*Data*[32]** (GDPR) daħal fis-seħħ fl-2016 u kien japplika minn Mejju 2018 'il quddiem. L-objettiv tiegħu

huwa li jipproteġi d-*data* personali taċ-ċittadini Ewropej billi jistabbilixxi regoli dwar l-ipproċessar u d-disseminazzjoni tagħha. Huwa jagħti lis-suġġetti tad-*data* ċerti drittijiet u jimponi obbligi fuq il-kontrolluri tad-*data* (fornituri ta' servizzi diġitali) rigward l-użu u t-trasferiment ta’ informazzjoni. Huwa jimponi wkoll rekwiżiti ta’ notifika f’każ ta’ ksur tar-regoli u, f’xi każijiet, jista’ jimponi multi. Il-***Figura 3*** turi kif id-Direttiva NIS u l-GDPR jikkomplementaw lil xulxin fl-għanijiet tagħhom biex isaħħu ċ-ċibersigurtà u jissalvagwardjaw il-protezzjoni tad-*data*.

22 Abbozz ta' leġiżlazzjoni li attwalment qed tiġi diskussa jinkludi l-Att propost dwar iċ-Ċibersigurtà biex isaħħaħ l-ENISA u jistabbilixxi mekkaniżmu ta’ ċertifikazzjoni għall-UE kollha[33], ir-regolament propost dwar l-ordnijiet ta’ produzzjoni u ta’ preservazzjoni għall-evidenza elettronika[34], u d-direttiva proposta dwar l-evidenza elettronika[35]. Il-Proposta tal-2018 għal Ċentru Ewropew ta’ Kompetenza Industrijali, Teknoloġika u tar-Riċerka fil-qasam taċ-Ċibersigurtà u n-Netwerk ta’ Ċentri Nazzjonali ta’ Koordinazzjoni (minn hawn ’il quddiem imsejħa “netwerk ta’ ċentri ta’ kompetenza dwar iċ-ċibersigurtà u ta’ ċentru ta’ kompetenza tar-riċerka”) tifforma parti mill-pakkett dwar iċ-ċibersigurtà tal-2017[36].

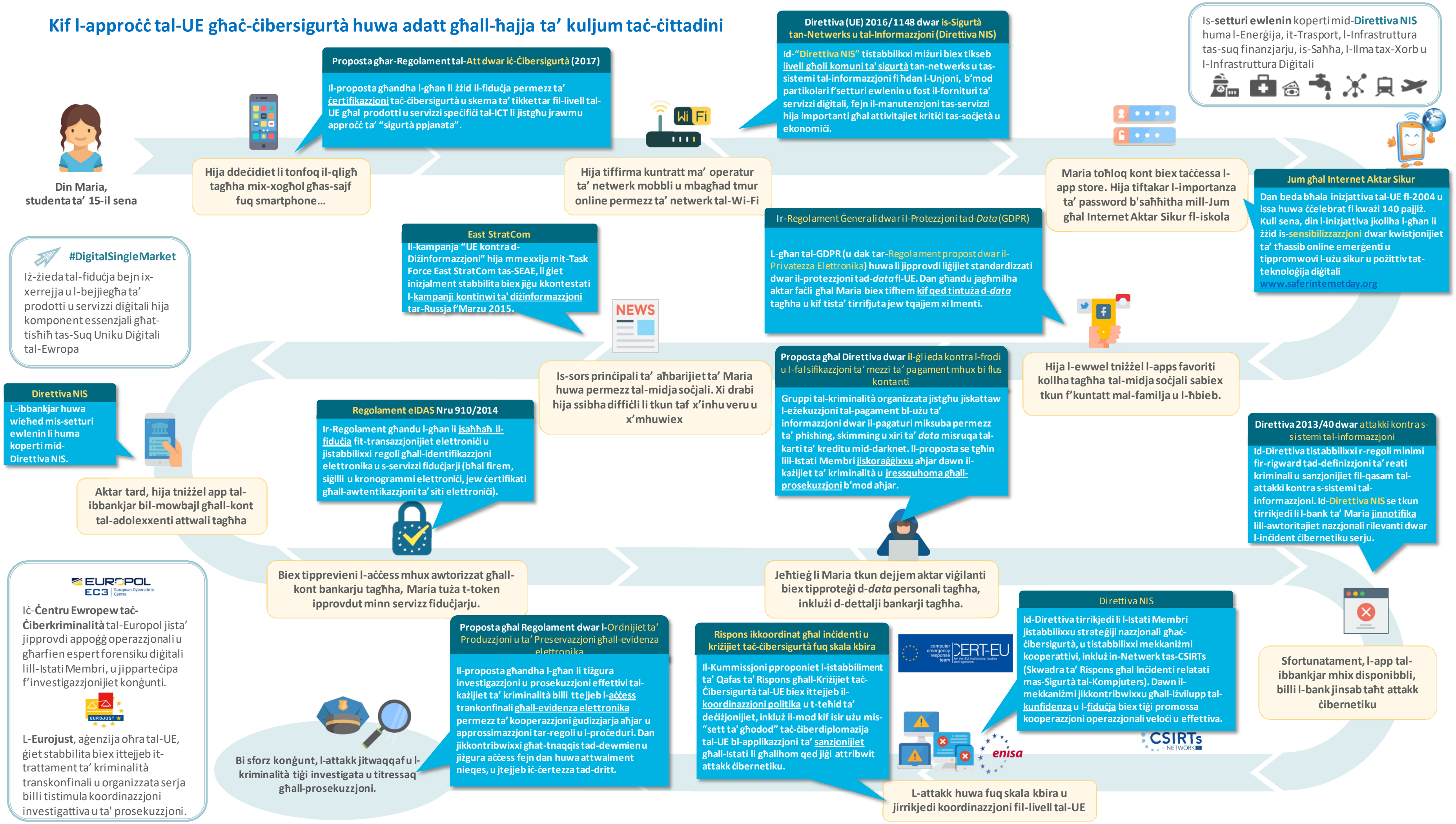
23 Jista’ jkun diffiċli li wieħed jifhem l-ambitu wiesa’ tal-qafas ta’ politika u leġiżlattiv li jirrigwarda ċ-ċibersigurtà u l-mod kif dan jaffettwa l-ħajja tagħna ta’ kuljum.

24 Il-***Figura 4*** tipprova tippreżenta l-intersezzjoni ta’ atti leġiżlattivi differenti u attivitajiet oħra mal-ħajja ta’ ċittadin Ewropew fittizju.

Figura 3 – Kif il-GDPR u d-Direttiva NIS jikkomplementaw lil xulxin

Sors: Il-QEA.

Figura 4 – Kif l-approċċ tal-UE għaċ-ċibersigurtà huwa adatt għall-ħajja ta' kuljum taċ-ċittadini



Sors: Il-QEA.

Kostruzzjoni ta’ qafas ta’ politika u leġiżlattiv

25 L-ekosistema ċibernetika tal-UE hija kumplessa u għandha diversi livelli, kif ukoll tinvolvi ħafna partijiet ikkonċernati (ara l-***Anness I***). It-tlaqqigħ flimkien tal-partijiet differenti kollha tagħha jippreżenta sfida konsiderevoli. Mill-2013 'il hawn, kien hemm motivazzjoni kkonċertata biex ikun hemm koerenza fil-qasam taċ-ċibersigurtà tal-UE[37].

Sfida 1: evalwazzjoni u obbligu ta’ rendikont siewja

26 Kif osservat il-Kummissjoni, huwa diffiċli li tiġi stabbilita relazzjoni kawżali bejn l-istrateġija tal-2013 u kwalunkwe bidla misjuba. L-objettivi ta’ din l-istrateġija ġew iffurmulati b’mod wiesa’ ħafna, u jesprimu viżjoni aktar milli mira li tista’ titkejjel[38]. L-iżvilupp ta’ azzjoni li hija allinjata ma’ dawn l-għanijiet wisgħin mhuwiex faċli fin-nuqqas ta’ objettivi li jistgħu jitkejlu. Il-qafas ta’ politika aġġornat dwar iċ-ċiberdifiża (2018) se jimmira li jiżviluppa objettivi li jistabbilixxu l-livell minimu ta’ ċibersigurtà u ta’ fiduċja li għandha tinkiseb. Madankollu, dan se jkun limitat għaċ-ċiberdifiża; ma ġewx stabbiliti objettivi li jiddefinixxu l-livell mixtieq ta’ reżiljenza għall-UE fl-intier tagħha.

27 L-eżiti rarament jitkejlu u huma ftit l-oqsma ta' politika li ġew evalwati[39]. Dan huwa parzjalment dovut għall-implimentazzjoni reċenti ta’ ħafna mill-miżuri – leġiżlattivi jew ta' natura oħra – li xxekkel it-twettiq ta’ evalwazzjoni sħiħa tal-impatt tagħhom. L-sfida hija li jiġu ddefinti kriterji ta’ valutazzjoni siewja li jistgħu jippermettu l-kejl tal-impatt tagħhom. Barra dan, evalwazzjoni rigoruża għadha ma saritx in-norma għaċ-ċibersigurtà b’mod ġenerali. Għalhekk, tinħtieġ bidla lejn kultura tal-prestazzjoni li tinkorpora prattiki ta’ evalwazzjoni u rappurtar standardizzat. Il-mandat attwali tal-ENISA ma jestendix sal-evalwazzjoni u l-monitoraġġ tal-istat taċ-ċibersigurtà u l-livell ta' tħejjija tal-UE.

28 It-tfassil tal-politika bbażat fuq l-evidenza jiddependi fuq id-disponibbiltà ta’ *data* u statistika affidabbli suffiċjenti bħala għajnuna għall-monitoraġġ u l-analiżi ta’ xejriet u ħtiġijiet. Ma hemmx biżżejjed *data* affidabbli minħabba n-nuqqas ta’ sistema obbligatorja u komuni ta’ monitoraġġ. L-indikaturi spiss ma jkunux faċilment disponibbli u huma diffiċli li jiġu ddefiniti[40]. Madankollu, f’xi oqsma ġiet żviluppata metrika speċifika, bħaċ-Ċiklu ta' Politika tal-UE, li tintuża biex tiġi indirizzata l-kriminalità serja u organizzata.

29 Ftit Stati Membri jiġbru b'mod regolari *data* uffiċjali dwar kwistjonijiet ċibernetiċi, u dan ixekkel il-komparabbiltà. L-UE sa issa tat ftit indikazzjoni dwar il-ħtieġa li tiġi kkonsolidata statistika fil-livell Ewropew[41]. Hemm ukoll ftit analiżijiet indipendenti mill-UE kollha li huma disponibbli u li jkopru suġġetti ewlenin bħal[42]: l-ekonomija taċ-ċibersigurtà, inklużi aspetti relatati mal-imġiba (allinjament ħażin tal-inċentivi, assimetriji tal-informazzjoni); il-fehim tal-impatt ta' fallimenti ċibernetiċi u taċ-ċiberkriminalità; makrostatistika dwar ix-xejriet ċibernetiċi u l-isfidi mistennija; u l-aħjar soluzzjonijiet biex jiġi indirizzat it-theddid.

30 Fid-dawl tan-nuqqas ta' objettivi speċifiċi u l-iskarsezza ta' *data* affidabbli u ta' indikaturi ddefiniti tajjeb, il-valutazzjoni tal-kisbiet tal-istrateġija kienet, sa issa, fil-biċċa l-kbira kwalitattiva. Ir-rapporti ta' progress spiss jiddeskrivu l-attivitajiet imwettqa jew l-istadji importanti miksuba, mingħajr kejl bir-reqqa tar-riżultati. Barra dan, il-linji bażi għall-valutazzjoni tar-reżiljenza tas-sistemi għadhom ma ġewx stabbiliti. Barra minn hekk, minħabba n-nuqqas ta' definizzjoni kodifikata ta' ċiberkriminalità huwa kważi impossibbli li jinstabu indikaturi rilevanti Ewropej li jgħinu fil-monitoraġġ u l-evalwazzjoni.

31 Is-sorveljanza indipendenti tal-implimentazzjoni tal-politika fil-qasam taċ-ċibersigurtà tvarja fost l-Istati Membri. Aħna stħarriġna l-uffiċċji nazzjonali tal-awditjar dwar l-esperjenza tagħhom fl-awditjar ta' dan il-qasam. Nofs ir-rispondenti kollha[43] qatt ma kienu awditjaw il-qasam. Għal dawk li kienu għamlu dan, il-fokus prinċipali kien fuq: il-governanza tal-informazzjoni, il-protezzjoni tal-infrastruttura kritika, l-iskambju ta' informazzjoni u l-koordinazzjoni fost il-partijiet ikkonċernati ewlenin; it-tħejjija, in-notifika u r-rispons għall-inċidenti. Fost is-suġġetti inqas koperti kien hemm miżuri ta' żieda tas-sensibilizzazzjoni u d-diskrepanza fil-ħiliet diġitali. Ir-riżultati ta' dawn l-awditi jew l-evalwazzjonijiet mhux dejjem jiġu ppubblikati għal raġunijiet ta' sigurtà nazzjonali. Lista ta' rapporti tal-awditjar ippubblikati mill-uffiċċji nazzjonali tal-awditjar hija inkluża fl-***Anness III***.

32 Il-limitazzjonijiet fil-ħiliet ċibernetiċi (ara wkoll il-paragrafi ***82 sa 90***) u d-diffikultajiet fl-evalwazzjoni tal-progress fil-qasam taċ-ċibersigurtà ġew ipperċepiti bħala l-isfidi prinċipali għall-awditjar ta' miżuri tal-gvern f'dan il-qasam.

Sfida 2: indirizzar tal-lakuni fid-dritt tal-UE u t-traspożizzjoni mhux uniformi tiegħu

33 Il-veloċità li biha jitfaċċaw teknoloġiji u theddid ġodda, hija ferma ktar rapida mit-tfassil u l-implimentazzjoni tal-leġiżlazzjoni tal-UE. Il-proċeduri tal-Unjoni ma tfasslux

bil-ħsieb tal-era diġitali: l-iżvilupp ta' proċeduri innovattivi u flessibbli biex jiġi żgurat qafas ta' politika u legali li jkun adatt għall-iskop[44] għal antiċipazzjoni u formulazzjoni aħjar tal-futur, huwa prijorità kritika[45].

34 Minkejja motivazzjoni għal koerenza akbar, il-qafas leġiżlattiv għaċ-ċibersigurtà jibqa' inkomplet (għal xi eżempji, ara t-*Tabella 1*). Il-frammentazzjoni u l-lakuni jxekklu l-ilħuq tal-objettivi kumplessivi ta' politika u jwasslu għal ineffiċjenzi. Il-lakuni li ġew identifikati mill-Kummissjoni fil-valutazzjoni tal-istrateġiji kienu jinkludu l-Internet tal-Oġġetti, il-bilanċ tar-responsabbiltajiet bejn l-utenti u l-fornituri ta' prodotti diġitali, kif ukoll ċerti aspetti li baqgħu ma ġewx indirizzati mid-Direttiva NIS. L-Att propost dwar iċ-Ċibersigurtà jipprova jindirizza dan parzjalment bil-promozzjoni ta' sigurtà ppjanata permezz ta' skema ta' ċertifikazzjoni għall-UE kollha. Xi partijiet ikkonċernati jemmnu li politika industrijali ċibernetika u approċċ komuni għaċ-ċiberspjunaġġ iddefiniti b'mod ċar għadhom notevolment neqsin[46].

Tabella 1 – Lakuni u traspożizzjoni mhux uniformi fil-qafas leġiżlattiv (mhux eżawrjenti)

Suq Uniku Diġitali	o Id-Direttiva attwali dwar il-Bejgħ lill-Konsumatur ma tkoprix iċ-ċibersigurtà. Id-direttivi proposti dwar il-kontenut diġitali[47] u l-bejgħ online[48] għandhom l-għan li jindirizzaw din id-diskrepanza. o Hemm oqfsa legali limitati u diversi għal dmirijiet ta' diliġenza fl-Istati Membri tal-UE, u dan iwassal għal inċertezza u diffikultà legali fl-infurzar ta’ rimedji legali[49]. o Politiki dwar id-divulgazzjonijiet tal-vulnerabbiltajiet tas-software qed jiġu żviluppati b’veloċitajiet differenti fl-Istati Membri kollha, mingħajr l-ebda qafas legali globali fil-livell tal-UE, biex jippermettu approċċ ikkoordinat[50].
Tisħiħ tas-sigurtà tan-netwerks u tal-informazzjoni	o L-Istati Membri huma liberi li jinkludu setturi li tħallew barra mid-Direttiva NIS[51]. L-industriji tal-akkomodazzjoni, li mhumiex koperti, jistgħu jagħtu aċċess għal każijiet oħra ta’ kriminalità, inkluż it-traffikar tal-bnedmin u tad-droga kif ukoll l-immigrazzjoni illegali[52].
Ġlieda kontra ċ-ċiberkriminalità	o Ħafna Stati Membri ma ddefinewx l-evidenza elettronika fil-leġiżlazzjoni nazzjonali tagħhom[53] (ara wkoll il-paragrafu ***22***). o Id-deċiżjoni qafas attwali dwar il-frodi permezz ta’ pagamenti mhux bi flus kontanti ma tinkludix b'mod espliċitu strumenti ta' pagament mhux fiżiċi bħal muniti virtwali, flus elettroniċi u trasferimenti ta’ flus permezz tal-mowbajl (mobile money), u lanqas ma tkopri dawn l-atti bħal phishing, skimming kif ukoll il-pussess u l-kondiviżjoni tal-informazzjoni dwar il-pagaturi[54]. o Id-Direttiva dwar l-Attakki kontra s-Sistemi tal-Informazzjoni ma tindirizzax b’mod dirett l-akkwiżizzjoni ta’ *data* illegali minn ġewwa (eż. Ċiberspjunaġġ), u dan iwassal għal sfidi għall-infurzar tal-liġi[55]. o Wara s-sentenza tal-Qorti tal-Ġustizzja tal-Unjoni Ewropea dwar iż-żamma ta’ *data*[56], id-differenzi fl-applikazzjoni tal-qafas legali fost l-Istati Membri impedixxew l-infurzar tal-liġi, li potenzjalment jirriżulta fit-telf ta’ ħjiel investigattiv u jxekkel il-prosekuzzjoni effettiva ta’ attività kriminali online[57].

Sors: Il-QEA.

35 L-applikazzjoni ta' xi aspetti tal-leġiżlazzjoni tibqa' volontarja kemm għall-awtoritajiet nazzjonali kif ukoll għall-operaturi privati. Pereżempju, fi ħdan il-qafas tal-Grupp ta' Kooperazzjoni, l-evalwazzjoni tal-istrateġiji nazzjonali dwar is-sigurtà tan-networks u tas-sistemi ta' informazzjoni kif ukoll l-effettività tas-CSIRTs hija volontarja. Barra minn hekk, taħt l-iskema ta' ċertifikazzjoni proposta fl-Att dwar iċ-Ċibersigurtà, l-applikazzjoni taċ-ċertifikazzjoni għal prodotti u servizzi tal-ICT tkun volontarja.

36 Fl-UE, iċ-ċibersigurtà hija prerogattiva tal-Istati Membri. Minkejja dan, l-UE għandha rwol kruċjali fil-ħolqien tal-kundizzjonijiet biex l-Istati Membri tagħha jtejbu l-kapaċitajiet tagħhom, u biex huma jaħdmu flimkien u jiġġeneraw il-fiduċja. Madankollu, minħabba d-differenzi kbar fost l-Istati Membri f'termini ta' kapaċità u involviment[58], il-provvediment ta' informazzjoni (tas-sigurtà nazzjonali) sensittiva se tibqa' volontarja.

37 It-traspożizzjoni inkonsistenti tad-dritt tal-UE fost l-Istati Membri tista' tirriżulta f'inkoerenza legali u operazzjonali, u ma tħallix il-leġiżlazzjoni tilħaq il-potenzjal sħiħ tagħha. Pereżempju, l-Istati Membri għandhom interpretazzjonijiet differenti ta' kif il-kontroll tal-esportazzjoni ta' oġġetti b'użu doppju għandhom jiġu applikati[59], bir-riżultat li xi kumpaniji bbażati fl-UE jistgħu jkunu qed jesportaw teknoloġiji u servizzi li jistgħu jintużaw għas-sorveljanza ċibernetika u għall-ksur tad-drittijiet tal-bniedem permezz ta' ċensura jew interċettazzjoni. Il-Parlament Ewropew esprima tħassib dwar dan[60].

38 Barra minn hekk, il-protezzjoni tal-privatezza u l-libertà ta' espressjoni tappella għal rispons leġiżlattiv speċjalizzat sabiex jinkiseb il-bilanċ meħtieġ bejn il-protezzjoni tal-valuri fundamentali u l-ksib tal-imperattivi tas-sigurtà tal-UE. Pereżempju, aħna kif niżguraw kriptaġġ minn tarf sa tarf filwaqt li nsibu l-aħjar mod kif nappoġġaw l-infurzar tal-liġi? Jew, kif nistgħu nilħqu l-għanijiet tal-GDPR filwaqt li nifhmu l-implikazzjonijiet tiegħu dwar informazzjoni disponibbli għall-pubbliku dwar ir-reġistranti ta' ismijiet tad-dominji u d-detenturi ta' blokki ta' indirizzi IP? U dan kif jista' jaffettwa b'mod negattiv l-investigazzjonijiet tal-infurzar tal-liġi[61]?

39 Il-leġiżlazzjoni waħidha ma tiggarantix ir-reżiljenza. Filwaqt li l-objettiv tad-Direttiva NIS huwa li tilħaq livell għoli ta' sigurtà madwar l-UE, hija tiffoka b'mod espliċitu fuq il-ksib ta' armonizzazzjoni minima, mhux massima[62]. Lakuni se jkomplu jitifaċċaw hekk kif ix-xenarju ċibernetiku jevolvi.

Punti ta' riflessjoni – qafas ta' politika

- X'passi kritiċi huma meħtieġa biex titqanqal bidla kemm minn dawk inkarigati mit-tfassil tal-politika kif ukoll mil-leġiżlaturi lejn kultura tal-prestazzjoni aktar b'saħħitha fil-qasam taċ-ċibersigurtà, inkluża d-definizzjoni ta' reżiljenza globali?

- Ir-riċerka kif tista' tikkontribwixxi aħjar għall-ġenerazzjoni tad-*data* u l-istatistika meħtieġa biex tkun tista' titwettaq evalwazzjoni siewja?

- B'liema modi l-proċessi leġiżlattivi tal-UE jistgħu jiġu adattati biex ikunu aktar flessibbli u jieħdu kont aħjar tal-veloċità tal-iżviluppi teknoloġiċi u dawk tat-theddid?

- Il-prattika ta' metrika li qed tiżviluppa (indikaturi, miri) fiċ-Ċiklu ta' Politika tal-UE kif tista' tiġi adattata, tiżdied u tiġi replikata għad-dominju taċ-ċibersigurtà fl-intier tiegħu?

- L-uffiċċji nazzjonali tal-awditjar x'jistgħu jitgħallmu mill-approċċi ta' xulxin għall-awditjar ta' politiki u miżuri ta' ċibersigurtà?

- Liema inkonsistenzi fit-traspożizzjoni u fl-implimentazzjoni tal-qafas legali tal-UE qed idgħajfu rispons aktar effettiv għal-lakuni relatati maċ-ċibersigurtà u maċ-ċiberkriminalità, u dan kif jista' jiġi indirizzat l-aħjar mill-Istati Membri u mill-istituzzjonijiet tal-UE?

- Kemm huma effettivi l-kontrolli tal-esportazzjoni tal-UE fuq prodotti u servizzi ċibernetiċi fil-prevenzjoni ta' abbuż tad-drittijiet tal-bniedem barra mit-territorju tal-UE?

Finanzjament u nfiq

40 L-UE għandha l-għan li ssir l-ambjent online l-aktar sikur fid-dinja. Il-ksib ta' din l-ambizzjoni jirrikjedi sforzi sinifikanti mill-partijiet ikkonċernati kollha, inkluża bażi finanzjarja soda u mmaniġġjata tajjeb.

Sfida 3: allinjament tal-livelli ta' investiment mal-għanijiet

Żieda tal-investiment

41 L-infiq totali globali għaċ-ċibersigurtà bħala perċentwal tal-PDG huwa stmat li huwa madwar 0.1 %. Fl-Istati Uniti[63], dan jiżdied għal madwar 0.35 % (inkluż is-settur privat). Bħala perċentwal tal-PDG, l-infiq tal-gvern federali tal-Istati Uniti huwa madwar 0.1 %, jew madwar USD 21 biljun ibbaġitajti għall-2019[64].

42 Bi tqabbil ma' dan, l-infiq fl-UE kien baxx, frammentat u spiss mhux sostnut minn programmi kkonċertati mmexxija mill-gvernijiet. Iċ-ċifri huma diffiċli biex jinkisbu, iżda l-infiq pubbliku tal-UE fuq iċ-ċibersigurtà huwa stmat li jvarja bejn EUR 1 biljun u EUR 2 biljun kull sena[65]. Xi nfiq tal-Istati Membri bħala perċentwal tal-PDG huwa wieħed minn kull għaxra tal-livelli tal-Istati Uniti, jew anke inqas[66]. Jeħtieġ li l-UE u l-Istati Membri jkunu jafu kemm qed jinvestu fondi kollettivament biex ikunu jafu liema lakuni għandhom jimlew.

43 Huwa diffiċli li tiġi ffurmata stampa komprensiva fin-nuqqas ta' *data* ċara minħabba n-natura trażversali taċ-ċibersigurtà u minħabba li l-infiq fuq iċ-ċibersigurtà u l-infiq ġenerali fl-IT huma spiss indistingwibbli[67]. L-istħarriġ tagħna kkonferma li huwa diffiċli li tinkiseb statistika affidabbli dwar l-infiq kemm fis-settur pubbliku kif ukoll f'dak privat. Tliet kwarti tal-uffiċċji nazzjonali tal-awditjar irrappurtaw li ma kellhomx stampa ġenerali ċentralizzata tal-infiq pubbliku ċibernetiku, u l-ebda wieħed mill-Istati Membri ma obbliga lill-entitajiet pubbliċi biex jirrappurtaw l-infiq fuq iċ-ċibersigurtà b'mod separat fil-pjanijiet finanzjarji tagħhom.

44 Iż-żieda tal-investiment pubbliku u dak privat f'ditti taċ-ċibersigurtà fl-Ewropa tippreżenta sfida partikolari. Il-kapital pubbliku huwa spiss disponibbli għall-fażijiet inizjali, iżda inqas disponibbli għall-istadji tat-tkabbir u l-espansjoni[68]. Jeżistu bosta inizjattivi ta' finanzjament tal-UE iżda mhux qed jittieħed vantaġġ minnhom, fil-biċċa l-kbira minħabba l-burokrazija[69]. B'mod kumplessiv, il-prestazzjoni tad-ditti taċ-ċibersigurtà fl-UE mhix tajba meta mqabbla ma' dik tal-pari internazzjonali tagħhom:

għadd inqas, l-ammont medju ta' finanzjament li jiġġeneraw huwa sinifikattivament aktar baxx[70]. L-iżgurar ta' mmirar u finanzjament effettiv tan-negozji li jkunu għadhom kemm jifthu huwa għalhekk kruċjali biex jintlaħqu l-objettivi tal-politika diġitali tal-UE.

Żieda tal-impatt

45 Jeħtieġ li t-tnaqqis tad-diskrepanza fl-investiment ċibernetiku jipprovdi eżiti utli. Pereżempju, minkejja s-saħħa tas-settur tar-riċerka u l-innovazzjoni tal-UE, ir-riżultati mhumiex koperti minn privattivi, ikkummerċjalizzati jew żviluppati biżżejjed biex jikkontribwixxu għat-tisħiħ tar-reżiljenza, il-kompetittività u l-awtonomija diġitali[71]. Dan huwa partikolarment il-każ meta mqabbel ma' dak tal-kompetituri globali tal-UE. L-insuffiċjenza ta' riżultati kkontrollati tajjeb tirriżulta minn firxa ta' fatturi[72], inklużi:

- in-nuqqas ta' strateġija transnazzjonali konsistenti għat-titjib tal-approċċ biex jissodisfa l-ħtiġijiet diġitali usa' tal-UE għall-kompetittività u l-awtonomija miżjuda;
- it-tul taċ-ċiklu tal-katina tal-valur, li jfisser li l-għodod dalwaqt se jsiru obsoleti;
- in-nuqqas ta' sostenibbiltà billi l-proġetti tipikament jintemmu bix-xoljiment tat-tim tal-proġetti u bil-waqfien tal-appoġġ, inklużi aġġornamenti u soluzzjonijiet bl-użu ta' software korrettiv.

46 Il-proposta tal-Kummissjoni biex jiġi stabbilit netwerk ta' ċentri ta' kompetenza dwar iċ-ċibersigurtà u ta' ċentru ta' kompetenza tar-riċerka hija tentattiv biex tingħeleb il-frammentazzjoni fil-qasam ta' riċerka dwar iċ-ċibersigurtà u biex jiġi stimulat aktar l-investiment f'dan il-livell[73]. B'kollox, hemm madwar 665 ċentru ta' għarfien espert madwar l-UE.

Sfida 4: stampa ġenerali ċara tal-infiq tal-baġit tal-UE

47 Stampa ġenerali ċentralizzata tal-infiq hija importanti għat-trasparenza u l-koordinazzjoni mtejba. Mingħajrha, huwa diffiċli għal dawk inkarigati mit-tfassil tal-politika li jaraw kif l-infiq ikun allinjat mal-ħtiġijiet biex jiġu ssodisfati l-għanijiet ta' prijorità.

48 Ma hemmx baġit iddedikat li jiffinanzja l-istrateġija għaċ-ċibersigurtà. Fil-livell tal-UE, l-infiq fuq iċ-ċibersigurtà, minflok, jiġi mill-baġit ġenerali tal-UE u mill-kofinanzjament mill-Istati Membri. L-analiżi tagħna tiżvela struttura kumplessa ta' mill-inqas 10 strumenti differenti taħt il-baġit ġenerali tal-UE, iżda ma tagħtix stampa ċara tal-fondi investiti u tal-iskop tagħhom (ara l-***Anness II***).

49 L-istabbiliment ta’ stampa ċara tal-infiq ta’ suġġett li jkopri firxa ta’ ħafna oqsma ta' politika huwa għaldaqstant sfida mdaqqsa. Il-programmi ta’ nfiq huma mmaniġġjati minn partijiet differenti tal-Kummissjoni, kull waħda bl-għanijiet, bir-regoli u bl-iskedi ta' żmien proprji tagħha. L-istampa hija aktar ikkumplikata meta jittieħed inkunsiderazzjoni l-kofinanzjament mill-Istati Membri, bħal taħt il-Fond għas-Sigurtà Interna (Pulizija)[74].

Infiq fuq iċ-ċibersigurtà li huwa identifikabbli

50 Fil-perjodu 2014 – 2018, il-Kummissjoni nefqet mill-inqas EUR 1.4 biljun fl-implimentazzjoni tal-Istrateġija[75], fejn allokat l-akbar sehem għal Orizzont 2020[76] (“H2020”). Il-finanzjament taħt H2020 jingħadda prinċipalment permezz tal-Programm għal Soċjetà Sigura u fit-Tmexxija biex ikunu jistgħu jitwettqu proġetti ta’ teknoloġija industrijali[77]. Sa Settembru 2018, aħna identifikajna 279 proġett relatati maċ-ċibersigurtà li ġew ikkuntrattati, b’finanzjament totali mill-UE li jammonta għal EUR 786 miljun[78]. Il-***Figura 5*** turi t-tipoloġija ta’ dawn il-proġetti abbażi ta’ din l-analiżi.

Figura 5 – Proġetti ta’ riċerka dwar iċ-ċibersigurtà li ġew ikkuntrattati taħt H2020 (EUR miljuni)

Sors: Il-QEA.

51 Fl-2016, ġiet stabbilita sħubija pubblika-privata kuntrattwali (cPPP) biex tistimula l-industrija Ewropea taċ-ċibersigurtà. L-għan kien li, sal-2020, jingħaddu EUR 450 miljun mill-Programm H2020 fis-cPPP u jiġi attirat ammont addizzjonali ta' EUR 1.8 biljun mis-settur privat. Fil-perjodu ta' 18-il xahar sal-31 ta' Diċembru 2017, EUR 67.5 miljun ingħaddew minn H2020 fis-cPPP u s-settur privat investa EUR 1 biljun[79].

52 Il-ġlieda kontra ċ-ċiberkriminalità hija appoġġata wkoll mill-Fond għas-Sigurtà Interna – Pulizija (FSI-P). Dan il-fond jappoġġa studji, laqgħat tal-esperti, u attivitajiet ta' komunikazzjoni; dawn ammontaw għal kważi EUR 62 miljun bejn l-2014 u l-2017. Barra dan, l-Istati Membri jistgħu jirċievu għotjiet għal tagħmir, taħriġ, riċerka u ġbir tad-*data* taħt ġestjoni kondiviża. Kien hemm 19-il Stat Membru li użaw dawn l-għotjiet għal EUR 42 miljun.

53 Il-fondi li jappoġġaw il-kooperazzjoni ġudizzjarja u l-funzjonament ta' trattati ta' għajnuna legali reċiproka, b'fokus speċifiku fuq l-iskambju ta' *data* elettronika u ta' informazzjoni finanzjarja, ammontaw għal EUR 9 miljun taħt il-Programm dwar il-Ġustizzja mmaniġġjat mid-DĠ JUST.

54 Id-Direttiva NIS tiddikjara b'mod espliċitu li s-CSIRTs irid ikollhom riżorsi adegwati biex iwettqu b'mod effettiv il-kompiti tagħhom[80]. Bejn l-2016 u l-2018, kienu disponibbli EUR 13-il miljun kull sena mill-Faċilità Nikkollegaw l-Ewropa, li għaliha l-Istati Membri setgħu japplikaw biex jgħinu l-implimentazzjoni tar-rekwiżiti tad-Direttiva. Ma kien hemm l-ebda studju li jiddetermina l-ħtiġijiet finanzjarji reali għan-netwerk tas-CSIRTs u l-Grupp ta' Kooperazzjoni biex ikollhom impatt.

55 Bosta spejjeż operazzjonali tal-aġenziji kienu mmirati speċifikament lejn iċ-ċibersigurtà jew l-attivitajiet ta' ċiberkriminalità. Huwa diffiċli, madankollu, li jiġu estratti xi ċifri eżatti mill-informazzjoni pubblika disponibbli.

56 Il-Konvenzjoni ta' Budapest (ara l-paragrafu ***11***) iffurmat il-pedament għall-infiq ċibernetiku estern tal-UE. L-UE nefqet madwar EUR 50 miljun biex issaħħaħ iċ-ċibersigurtà lil hinn mill-fruntieri tagħha fil-perjodu 2014-2018. Kważi nofs dan l-ammont kien permezz tal-istrument li jikkontribwixxi għall-Istabbiltà u l-Paċi, bi proġett prinċipali wieħed – il-GLACY+ b'ammont ta' EUR 13,5 miljun – li għandu l-għan li jsaħħaħ il-kapaċitajiet fid-dinja kollha biex tiġi żviluppata u implimentata l-leġiżlazzjoni dwar iċ-ċiberkriminalità u tiżdied il-kooperazzjoni internazzjonali[81]. Bnadi oħra, il-fokus tal-infiq minn strumenti finanzjarji oħra tal-UE kien fil-biċċa l-kbira fuq il-Balkani tal-Punent[82], kif ukoll fuq il-viċinat Ewropew, pereżempju l-proġett Cybercrime@EaP mal-

pajjiżi tas-Sħubija tal-Lvant għandu l-għan li jtejjeb il-kooperazzjoni internazzjonali dwar iċ-ċiberkriminalità u l-evidenza elettronika.

Infiq ieħor fuq iċ-ċibersigurtà

57 Mhux dejjem ikun possibbli li jiġi identifikat infiq speċifiku fuq iċ-ċibersigurtà fi ħdan il-programmi tal-UE:

- il-finanzjament taħt H2020 ukoll ingħadda permezz tal-impriża konġunta Komponenti u Sistemi Elettroniċi għat-Tmexxija Ewropea (ECSEL) għal sistemi ċiberfiżiċi. Madankollu, aħna ma stajniex niddeterminaw x'kien speċifikament relatat maċ-ċibersigurtà minn fost is-27 proġett li kienu jammontaw għal total ta' EUR 437 miljun bejn l-2015 u l-2016.

- Sa EUR 400 miljun huma disponibbli għall-infiq fuq iċ-ċibersigurtà u s-servizzi fiduċjarji taħt il-Fondi Strutturali u ta' Investiment Ewropej. Dawn ikopru investimenti fis-sigurtà u fil-protezzjoni tad-*data* biex jissaħħu l-interoperabbiltà u l-interkonnessjoni ta' infrastruttura diġitali, l-identifikazzjoni elettronika, kif ukoll is-servizzi ta' privatezza u dawk fiduċjarji.

58 Fil-Pjan Operazzjonali 2018 tiegħu, il-Bank Ewropew tal-Investiment ħabbar l-intenzjoni tiegħu li jżid il-finanzjament tat-teknoloġija b'użu doppju, taċ-ċibersigurtà u tas-sigurtà ċivili għal sa EUR 6 biljun fuq perjodu ta' tliet snin[83].

Inħarsu 'l quddiem

59 Il-komponent taċ-ċibersigurtà b'ammont ta' EUR 2 biljun tal-Programm Ewropa Diġitali[84] (DEP) propost ġdid għall-perjodu 2021-2027 huwa mfassal biex isaħħaħ l-industrija taċ-ċibersigurtà tal-UE u l-protezzjoni kumplessiva tas-soċjetà, inkluż billi jagħti għajnuna għall-implimentazzjoni tad-Direttiva NIS. In-netwerk propost ta' ċentri ta' kompetenza dwar iċ-ċibersigurtà u ta' ċentru ta' kompetenza tar-riċerka, li għandu l-għan li jwassal għal approċċ aktar issimplifikat, huwa mistenni li jifforma l-mekkaniżmu prinċipali ta' implimentazzjoni għall-infiq tal-UE taħt id-DEP.

60 L-infiq fuq id-difiża mill-baġit tal-UE żdied dan l-aħħar permezz tal-Programm Ewropew għall-Iżvilupp fl-Industrija tad-Difiża, b'EUR 500 biljun li għandhom jiġu allokati fl-2019 u l-2020[85]. Dan se jiffoka fuq it-titjib tal-koordinazzjoni u l-effiċjenza tal-infiq fuq id-difiża min-naħa tal-Istati Membri permezz ta' inċentivi għall-iżvilupp konġunt. Wara l-2020, huwa għandu l-għan li jiġġenera investiment totali ta' EUR 13-

il biljun fil-kapaċità ta' difiża permezz tal-Fond Ewropew għad-Difiża, li ftit minnu jkopri ċ-ċiberdifiża[86].

Sfida 5: forniment ta' riżorsi adegwati għall-aġenziji tal-UE

61 It-tliet korpi fundamentali fil-qalba tal-politika tal-UE fil-qasam taċ-ċibersigurtà – l-ENISA, l-EC3 tal-Europol, u s-CERT-UE (ara l-***Kaxxa 2***) qed jiffaċċjaw sfidi relatati mal-forniment ta' riżorsi fi żmien ta' prijoritajiet politiċi intensifikati xprunati mis-sigurtà. L-allokazzjoni attwali ta' riżorsi umani u finanzjarji fl-aġenziji tal-UE tibqa' sfida għalihom biex jissodisfaw l-aspettattivi tagħhom[87].

62 It-talbiet tal-aġenziji għal riżorsi addizzjonali biex tiġi ssodisfata d-domanda dejjem tikber, ma ġewx issodisfati għalkollox, u dan jista' jipperikola l-issodisfar (f'waqtu) tal-objettivi tal-politika. Pereżempju:

- Riżorsi limitati kienu fattur li ma ħalliex lill-ENISA tilħaq kompletament l-objettivi tagħha fl-2017[88]. Riżorsi addizzjonali ġew proposti fil-pakkett tal-2017 biex jaqblu mal-mandat il-ġdid tal-ENISA.

- Il-forniment ta' analisti u ta' investiment fil-kapaċitajiet tal-ICT fl-EC3 tal-Europol ma laħħqux mad-domanda[89]. Barra minn hekk, il-persunal tat-Taskforce ta' Azzjoni Konġunta kontra ċ-Ċiberkriminalità (J-CAT) tal-EC3 tal-Europol jinkludi esperti mill-Istati Membri u minn pajjiżi terzi biex jappoġġaw investigazzjonijiet immexxija mill-intelligence. Iżda l-ispejjeż fil-biċċa l-kbira jiġġarrbu mill-Istati mittenti, u dan jiskoraġġixxi l-iskjerament ta' għedud akbar ta' esperti. Skjerament temporanju u skont il-każ tfassal b'xi finanzjament tal-Europol jew taċ-Ċiklu ta' Politika tal-UE biex jippermetti l-parteċipazzjoni minn aktar pajjiżi.

63 Xi limitazzjonijiet huma awtokaġunati. Ħafna membri tal-persunal fis-CERT-UE u fl-ENISA huma aġenti kuntrattwali, li l-proċeduri ta' reklutaġġ għalihom jimxu tipikament bil-mod. Oħrajn, bħall-attrazzjoni u ż-żamma ta' talent, jirriżultaw mill-inabbiltà tal-aġenziji li jikkompetu mas-salarji tas-settur privat jew minħabba prospetti baxxi għall-progressjoni tal-karrieri. Għalhekk, l-ENISA esternalizzat ħafna mix-xogħol tagħha bejn l-2014 u l-2016[90].

64 In-nuqqas ta' persunal u l-għodod meħtieġa jista' jinvolvi riskji sinifikanti, speċjalment rigward il-ġbir ta' intelligence dwar it-theddid. Il-volum ta' *data* minn sorsi miftuħa u dawk magħluqa qed ikompli jikber u għandu r-riskju li jegħleb il-kapaċitajiet tal-analisti li jwettqu analiżijiet xierqa tat-theddid. Mingħajr il-kapaċitajiet u l-għodod it-tajbin stabbiliti biex din id-*data* tiġi integrata u interkonnessa b'suċċess, hija ma tiġix

ikkonkretizzata b'mod effettiv f'intelligence utli dwar it-theddid li tista' tiġi kondiviża u analizzata fl-UE[91].

Punti ta' riflessjoni – Finanzjament u nfiq

- B'liema modi l-Kummissjoni u l-leġiżlaturi jistgħu jissimplifikaw l-infiq tal-UE fuq iċ-ċibersigurtà u b'mod aktar espliċitu jallinjawh ma' għanijiet iddefiniti b'mod ċar?
- In-nuqqasijiet fil-forniment ta' riżorsi tal-aġenziji tal-UE kif jistgħu jiġu indirizzati b'mod globali filwaqt li jittieħed kont tal-ħtiġijiet u l-għanijiet tal-Unjoni?
- X'miżuri qed jiġu identifikati fil-livell tal-UE u tal-Istati Membri biex jitnaqqsu l-ostakli għall-SMEs li qed jużaw il-kapital ta' investiment biex iżidu l-attivitajiet tagħhom?
- X'riżultati konkreti u sostnuti qed jagħtu l-fondi ta' H2020 biex jipproduċu soluzzjonijiet fir-rigward taċ-ċibersigurtà?
- L-eżerċizzji tal-UE għat-tisħiħ tal-kapaċitajiet kif qed isaħħu l-kapaċitajiet lil hinn mill-konfini tagħha f'konformità mal-valuri tal-UE?

Bini ta' soċjetà reżiljenti għaċ-ċibernetika

65 Il-governanza taċ-ċibersigurtà tittratta l-ġestjoni tat-theddid u r-riskji, it-tisħiħ tal-kapaċità u s-sensibilizzazzjoni, kif ukoll il-koordinazzjoni u l-kondiviżjoni tal-informazzjoni mibnija fuq pedament ta' fiduċja.

Sfida 6: tisħiħ tal-governanza u l-istandards

Governanza tas-sigurtà tal-informazzjoni

66 Il-governanza tas-sigurtà tal-informazzjoni hija dwar l-istabbiliment ta' strutturi u politiki biex jiġu żgurati l-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data*. Billi mhijiex sempliċiment kwistjoni teknika, hija tirrikjedi tmexxija effettiva, proċessi robusti u strateġiji allinjati mal-objettivi organizzattivi[92]. Subsett ta' din hija l-governanza taċ-ċibersigurtà, li tittratta t-tipi kollha ta' theddid ċibernetiku, inklużi attakki, ksur tar-regolamenti jew inċidenti mmirati u sofistikati li huma diffiċli li jiġu identifikati jew immaniġġjati.

67 Il-mudelli ta' governanza taċ-ċibersigurtà jvarjaw fost l-Istati Membri, u fi ħdanhom ir-responsabbiltà għaċ-ċibersigurtà hija spiss maqsuma fost ħafna entitajiet. Dawn id-differenzi jistgħu jostakolaw il-kooperazzjoni meħtieġa biex jingħata rispons għal inċidenti transkonfinali fuq skala kbira, kif ukoll biex tiġi skambjata intelligence dwar it-theddid fil-livell nazzjonali – u wisq inqas fil-livell tal-UE. L-istħarriġ li wettaqna tal-uffiċċji nazzjonali tal-awditjar żvela li dgħufijiet fl-arranġamenti ta' governanza u fil-ġestjoni tar-riskju tal-awtoritajiet pubbliċi ġew ipperċepiti bħala l-ogħla riskji.

68 Għalkemm il-konsegwenzi għall-organizzazzjonijiet tas-settur privat jistgħu jkunu severi, hemm għadd kbir ta' dgħufijiet fil-governanza tal-qasam taċ-ċiberspazju. Kważi 9 minn 10 organizzazzjonijiet jgħidu li l-funzjoni tagħhom fil-qasam taċ-ċibersigurtà ma tissodisfax għalkollox il-ħtiġijiet tagħhom[93], u l-uffiċjali taċ-ċibersigurtà spiss jitneħħew b'mill-inqas żewġ livelli mill-bord[94].

69 Id-direttivi tal-UE dwar il-liġi tal-kumpaniji ma jistabbilixxu l-ebda rekwiżit speċifiku dwar id-divulgazzjoni ta' riskji ċibernetiċi. Fl-Istati Uniti, il-Kummissjoni għat-Titoli u l-Kambju dan l-aħħar ħarġet gwida mhux vinkolanti biex tassisti lil kumpaniji pubbliċi fit-tħejjija ta' divulgazzjonijiet dwar ir-riskji u l-inċidenti relatati maċ-

ċibersigurtà[95]. Il-Kumitat Konġunt tal-Awtoritajiet Superviżorji Ewropej[96] (ASE) wissa dwar iż-żieda fir-riskji ċibernetiċi, ħeġġeġ lill-istituzzjonijiet finanzjarji biex itejbu s-sistemi fraġli tal-IT, u biex jesploraw ir-riskji inerenti għas-sigurtà tal-informazzjoni, il-konnettività u l-esternalizzazzjoni[97].

70 It-tisħiħ tal-governanza tas-sigurtà tal-informazzjoni tal-SMEs hija b'mod speċjali diffiċli peress li, ta' spiss, dawn ma jkunux jistgħu jimplimentaw is-sistemi xierqa. L-SMEs għandhom nuqqas ta' linji gwida adatti dwar l-applikazzjoni tas-sigurtà tal-informazzjoni u tar-rekwiżiti ta' privatezza kif ukoll il-mitigazzjoni ta' riskji teknoloġiċi[98]. Għalhekk, l-isfidi ewlenin huma l-fehim aħjar tal-ħtiġijiet tagħhom u l-provvedimemt tal-inċentivi u l-appoġġ meħtieġa.

71 In-nuqqas ta' qafas ta' governanza koerenti u internazzjonali għaċ-ċibersigurtà jxekkel l-abbiltà tal-komunità internazzjonali li tirreaġixxi għal ċiberattakki u li tillimitahom. Għalhekk, huwa importanti li jintlaħaq kunsens dwar dan il-qafas ta' governanza li jirrifletti bl-aħjar mod l-interessi u l-valuri tal-UE[99]. Tentattivi biex jiġu stabbiliti normi internazzjonali vinkolanti taċ-ċiberspazju qed isiru dejjem aktar riskjużi, kif jidher fin-nuqqas ta' kunsens fi ħdan il-Grupp ta' Esperti Governattivi tan-NU fl-2017 dwar kif id-dritt internazzjonali għandu japplika għar-rispons għal inċidenti min-naħa tal-Istati.

72 Biex issaħħaħ l-aġenda tagħha dwar il-governanza taċ-ċiberspazju, l-UE fformalizzat ukoll sitt sħubiji ċibernetiċi biex tistabbilixxi djalogi ta' politika regolari bl-għan li tibni fiduċja u oqsma komuni għall-kooperazzjoni[100]. L-eżiti huma mħallta; iżda, b'mod kumplessiv, fid-dominju internazzjonali, l-UE għadha ma tistax titqies li hija attur importanti taċ-ċibersigurtà, għalkemm saħħet il-profil tagħha[101].

Sigurtà tal-informazzjoni fl-istituzzjonijiet tal-UE

73 Kull istituzzjoni tal-UE għandha r-regoli proprji tagħha dwar il-governanza tas-sigurtà tal-informazzjoni. Ftehim interistituzzjonali jipprevedi assistenza relatata mas-sigurtà tal-informazzjoni mill-Kummissjoni għall-istituzzjonijiet u l-aġenziji l-oħra. L-istituzzjonijiet u l-korpi tal-UE rrikonoxxew il-ħtieġa li jiżviluppaw il-kapaċitajiet ċibernetiċi u l-approċċi għall-ġestjoni tar-riskju tagħhom b'mod koerenti. Fl-2020, il-Kummissjoni, il-Kunsill u s-SEAE għandhom jippreżentaw rapport lill-Grupp ta' Ħidma Orizzontali dwar Kwistjonijiet ta' Ċiberspazju dwar il-governanza u l-progress li sar fil-kjarifika u l-armonizzazzjoni tal-governanza taċ-ċibersigurtà fl-istituzzjonijiet u l-aġenziji tal-UE[102].

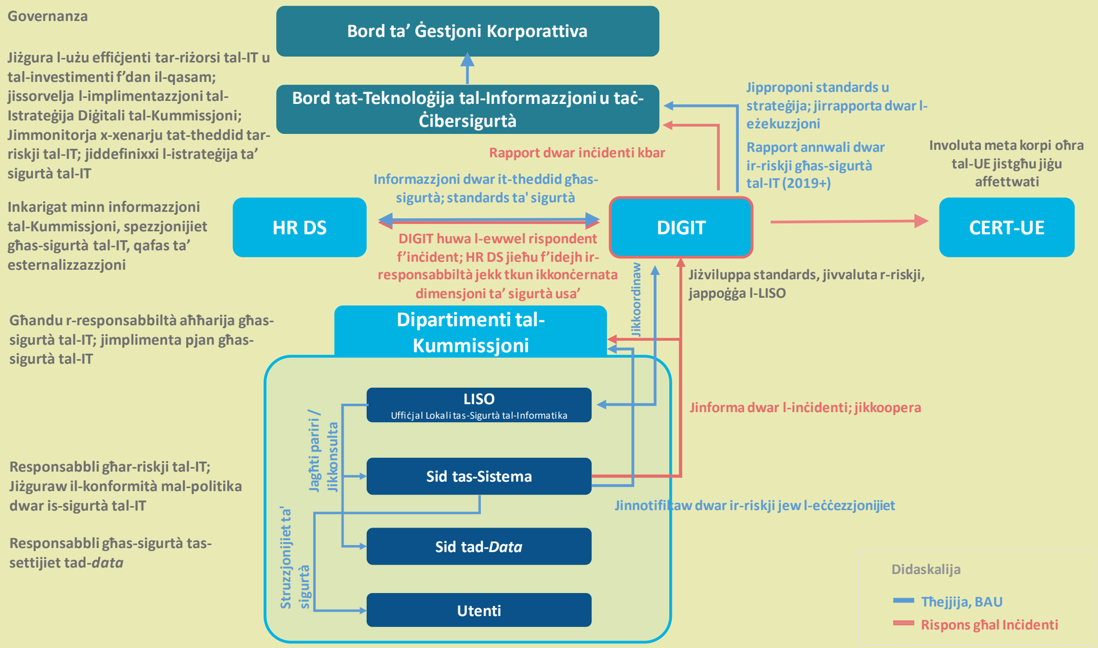
74 Fi ħdan il-Kummissjoni, id-Direttorat Ġenerali għall-Informatika (DIGIT) huwa responsabbli għas-sigurtà tal-infrastruttura u s-servizzi tal-IT (ara l-*Kaxxa 3*). L-objettivi prinċipali ta' sigurtà tal-IT tal-Istrateġija Diġitali tal-Kummissjoni qed jinkorporaw is-sigurtà tal-IT fil-proċessi ta' ġestjoni; il-provvediment ta' infrastruttura u reżiljenza (kost-) effettivi; it-twessigħ tal-ambitu tal-identifikazzjoni ta' inċidenti u r-rispons għalihom; u l-integrazzjoni tal-IT u l-governanza tas-sigurtà[103]. Il-Kummissjoni, taħt il-kuntratt tal-fornituri tagħha, tiżgura li kważi s-software kollu ssirlu manutenzjoni b'mod attiv, u li jintuża biss software appoġġat mill-bejjiegħ[104].

75 L-importanza tal-protezzjoni tal-istituzzjonijiet tasal ukoll sal-missjonijiet u l-istrutturi tal-PSDK tal-UE fid-dinja kollha. Waħda mill-prijoritajiet tal-Qafas ta' Politika tal-UE dwar iċ-Ċiberdifiża (aġġornament tal-2018) huwa li tissaħħaħ il-protezzjoni tas-sistemi tan-netwerks ta' komunikazzjoni u informazzjoni tal-PSDK li jintużaw minn entitajiet tal-UE. Bord intern tas-SEAE għall-Governanza tal-Qasam taċ-Ċiberspazju issa huwa stabbilit u ltaqa' għall-ewwel darba f'Ġunju 2017[105].

Kaxxa 3

Protezzjoni tas-sistemi ta' informazzjoni tal-Kummissjoni

Bejn wieħed u ieħor, 1 300 sistema u 50 000 apparat tal-Kummissjoni huma mmirati kontinwament minn ċiberattakki. Ir-responsabbiltà għall-IT hija deċentralizzata, kif jidher fil-figura hawn taħt. L-informazzjoni u s-sigurtà tal-IT huma bbażati fuq pjan komuni għas-sigurtà tal-IT stabbilit mid-DIGIT. Il-Bord tat-Teknoloġija tal-Informazzjoni u taċ-Ċibersigurtà jaġixxi bħala l-Uffiċjal Kap tas-Sigurtà tal-Informazzjoni *de facto* tal-Kummissjoni u jorbot il-lat operazzjonali tas-sigurtà tal-IT mal-maniġment superjuri tal-Kummissjoni, irrappreżentat mill-Bord ta' Ġestjoni Korporattiva.



Sors: Il-QEA, ibbażat fuq Deċiżjonijiet tal-Kummissjoni[106].

Il-kompitu prinċipali tad-DĠ Riżorsi Umani u Sigurtà (DĠ HR DS) huwa li jipproteġi lill-persunal, l-informazzjoni u l-assi tal-Kummissjoni. Huwa jwettaq ukoll investigazzjonijiet ta' sigurtà tal-inċidenti li għandhom dimensjoni ta' sigurtà usa' minn dawk tal-IT biss, għaldaqstant jikkontribwixxi għall-attivitajiet ta' kontrospjunaġġ u ta' kontra t-terroriżmu.

Id-DIGIT huwa responsabbli għas-sigurtà tal-IT u jospita s-CERT-UE (Skwadra ta' Rispons f'Emerġenza relatata mal-Kompjuters). Stabbilita fl-2011, is-CERT-UE topera b'baġit annwali ta' madwar EUR 2.5 miljun kull sena u għandha madwar 30 membru tal-persunal. Hija l-ewwel rispondent fi kwalunkwe inċident relatat mas-sigurtà tal-informazzjoni li jirrigwarda bosta istituzzjonijiet, iżda ma toperax fuq bażi ta' 24 siegħa kuljum. Hija tospita pjattaforma għall-kondiviżjoni tal-informazzjoni. Fl-2018, is-CERT-UE ffirmat memorandum ta' qbil mhux vinkolanti mal-ENISA, l-EC3 u l-Aġenzija Ewropea għad-Difiża biex issaħħaħ il-kooperazzjoni u l-koordinazzjoni. Hija għandha wkoll ftehim

tekniku mal-kapaċità ta' rispons tan-NATO għal inċidenti relatati mal-kompjuters (NCIRC).

Valutazzjonijiet tar-riskji u tat-theddid

76 Il-valutazzjonijiet tar-riskji u tat-theddid imsejsin fuq bażi soda u kontinwi huma għodod importanti kemm għall-organizzazzjonijiet pubbliċi kif ukoll dawk privati. Madankollu, ma hemm l-ebda approċċ standard għall-klassifikazzjoni u l-immappjar ta' theddid ċibernetiku jew għall-valutazzjonijiet tar-riskju, li jfisser li l-kontenut tal-valutazzjonijiet ivarja konsiderevolment, filwaqt li jippreżenta sfida għal approċċ koerenti għaċ-ċibersigurtà fil-livell tal-UE[107]. Barra dan, huma spiss iserrħu fuq l-istess sorsi jew anke fuq valutazzjonijiet oħra tat-theddid, b'hekk ma jkollhomx l-istampa kollha u jirriżultaw sejbiet ripetuti[108], bir-riskju li ma jagħtux attenzjoni biżżejjed lil theddid ieħor. Dan huwa aggravat minn nuqqas ta' rieda kontinwu għall-kondiviżjoni ta' informazzjoni u għan-nuqqas ta' rappurtar ta' inċidenti.

77 Iċ-Ċellola ta' Fużjoni kontra t-Theddid Ibridu[109], inkorporata fi ħdan is-SEAE, ġiet stabbilita biex ittejjeb l-għarfien tas-sitwazzjoni u tappoġġa t-teħid ta' deċiżjonijiet permezz ta' kondiviżjoni tal-analiżijiet, iżda jeħtieġ li din twessa' l-għarfien espert tagħha, inkluż fil-qasam taċ-ċibersigurtà. B'mod parallel, is-CERT-UE tipprovdi lill-istituzzjonijiet, il-korpi u l-aġenziji tal-UE rapporti u dokumenti ta' tgħarrif rigward it-theddid ċibernetiku mmirat lejhom.

78 Fil-passat, l-ENISA osservat li ħafna Stati Membri għandhom fehim kwalitattiv tat-theddid, u li hemm ħtieġa għal aktar immudellar ta' theddid ċibernetiku[110]. Il-kapaċità ta' monitoraġġ għall-analiżi strateġika ssaħħaħ il-fehim kumplessiv. Madankollu, il-valutazzjonijiet tat-theddid jistgħu jkopru mhux biss theddid teknoloġiku, iżda wkoll theddid soċjopolitiku u ekonomiku biex tiġi żgurata stampa aktar komprensiva, kif ukoll motivi tal-motivaturi u l-atturi tat-theddid.

Inċentivi

79 Xorta waħda għad hemm ftit wisq inċentivi legali u ekonomiċi biex l-organizzazzjonijiet jinnotifikaw u jikkondividu informazzjoni dwar l-inċidenti. Minħabba l-biża' ta' danni għar-reputazzjoni, ħafna organizzazzjonijiet xorta waħda jippreferu jittrattaw iċ-ċiberattakki b'mod diskret jew iħallsu lill-awturi. Għad irid jiġi stabbilit kemm id-Direttiva NIS tkun effettiva fiż-żieda tal-livell ta' notifiki. Il-Kummissjoni tistenna li t-titjib jimmaterjalizza primarjament fil-livell nazzjonali, iżda l-Att dwar iċ-Ċibersigurtà iżid perspettiva tal-UE kollha.[111]

80 Billi jinkorporaw ċerti standards fl-akkwist tiegħu, l-awtoritajiet pubbliċi għandhom ingranaġġ sinifikanti fuq il-fornituri bħala xerrejja ta' prodotti u servizzi diġitali permezz ta' akkwist pubbliku, kif ukoll il-finanzjament tar-riċerka u l-programmi (pereżempju, billi jirrikjedu l-adozzjoni ta' ċerti standards tekniċi bħall-Protokoll tal-Internet (IPv6) biex jikkontribwixxu għall-ġlieda kontra ċ-ċiberkriminalità). Madankollu, attawalment, ma hemm l-ebda qafas ta' akkwist konġunt għall-infrastruttura taċ-ċibersigurtà[112]. Hemm ħafna li l-Kummissjoni tista' tagħmel f'dan ir-rigward. Id-DEP propost għall-qafas finanzjarju pluriennali li jmiss għandu l-għan li jindirizza l-investiment mis-settur pubbliku, li sa issa kien limitat, fix-xiri tat-teknoloġija taċ-ċibersigurtà l-aktar reċenti.

81 Permezz tal-kapaċità regolatorja tagħha, il-Kummissjoni tista' tiżgura li l-istandards it-tajbin jiġu żviluppati għal adozzjoni mifruxa biex tissaħħaħ is-sigurtà. Il-Kummissjoni u l-Europol jaħdmu ma' korpi ta' governanza tal-Internet bħall-ICANN (ara l-paragrafu ***38***) u r-RIPE-NCC[113], li huwa essenzjali għall-istabbiliment tal-arkitettura t-tajba taċ-ċiberkriminalità biex jingħata appoġġ lill-awtoritajiet tal-infurzar tal-liġi u lil dawk ġudizzjarji.

Sfida 7: żieda tal-ħiliet u s-sensibilizzazzjoni

82 L-ENISA indikat li l-utenti għandhom rwol kruċjali fir-rigward taċ-ċiberattakki, u li t-tisħiħ tal-ħiliet, l-edukazzjoni u s-sensibilizzazzjoni huwa essenzjali għall-bini ta' soċjetà reżiljenti għaċ-ċibernetika[114]. Kemm jekk ikunu individwi, ix-xogħol jew id-dar, li huma kompetenti biex jagħrfu s-sinjali ta' twissija u armati bit-tekniki t-tajbin jistgħu jnaqqsu r-ritmu jew jipprevienu l-attakki.

83 Partikolarment preokkupanti hija l-asimetrija dejjem akbar bejn l-għarfien espert meħtieġ għat-twettiq ta' ċiberkriminalità jew it-tnedija ta' ċiberattakk, u l-ħiliet meħtieġa għad-difiża kontrih. Il-mudell ta' reat kriminali bħala servizz naqqas l-ostakli għad-dħul fis-suq ċiberkriminali: individwi mingħajr l-għarfien tekniku biex jibnuhom issa jistgħu jikru botnets, kitts ta' sfruttament jew pakketti dwar is-software ta' riskatt.

Taħriġ, ħiliet u żvilupp tal-kapaċitajiet

84 Id-dinja qed tiffaċċja nuqqas dejjem akbar ta' ħiliet fil-qasam taċ-ċibersigurtà; id-diskrepanza fil-forza tax-xogħol żdiedet b'20 % mill-2015 'il hawn[115]. Il-mezzi tradizzjonali ta' reklutaġġ mhumiex qed jissodisfaw id-domanda, inkluż għal pożizzjonijiet maniġerjali u interdixxiplinari[116]. Kważi 90 % tal-forza tax-xogħol globali

fil-qasam taċ-ċibersigurtà huma rġiel; in-nuqqas persistenti ta' diversità tal-ġeneru jkompli jillimita l-ġabra ta' talenti[117]. Barra dan, fl-universitajiet, is-suġġetti relatati mal-qasam ċibernetiku mhumiex irrappreżentati b'mod suffiċjenti fi programmi mhux tekniċi.

85 It-taħriġ u l-edukazzjoni huma meħtieġa fil-kategoriji kollha, fost l-impjegati taċ-ċivil, l-uffiċjali tal-infurzar tal-liġi, l-awtoritajiet ġudizzjarji, il-forzi armati u l-edukaturi. Pereżempju, jeħtieġ li l-qrati ġudizzjarji jkunu jistgħu jittrattaw il-partikolaritajiet tekniċi, li qed jinbidlu malajr, taċ-ċiberkriminalità u l-vittmi tagħha[118]; attwalment, ma hemmx standards fil-livell tal-UE għat-taħriġ u ċ-ċertifikazzjoni[119]. Fl-istituzzjonijiet tal-UE, huwa importanti li tinkiseb it-taħlita t-tajba ta' ħiliet. Mingħajr din, hemm il-possibbiltà li l-istituzzjonijiet jistgħu ma jkunux jistgħu jiddefinixxu l-ambitu b'mod xieraq, jidentifikaw is-sħab u l-ħtiġijiet ta' sigurtà t-tajbin, jew ma jkollhomx il-kapaċità li jimmaniġġjaw il-programmi. Min-naħa tiegħu, dan jista' jdgħajjef l-effettività tal-programmi jew l-iżvilupp tal-politika tal-UE.

86 Filwaqt li l-Istati Membri huma responsabbli għall-politiki tal-edukazzjoni fil-livell tal-UE, bosta attivitajiet ta' taħriġ (ara t-***Tabella 2***) u eżerċizzji (ara l-***Kaxxa 4***) diġà qed jiġu implimentati. L-UE tista' tikkontribwixxi biex l-istandards fil-livell tal-UE jiġu inkorporati fil-kurrikuli tat-tagħlim fid-dixxiplini rilevanti kollha[120]. Fil-qasam tal-forensika diġitali, pereżempju, standards komuni ta' taħriġ huma meħtieġa biex jiffaċilitaw it-triq għall-ammissibbiltà tal-evidenza fl-Istati Membri. Minħabba n-natura transkonfinali taċ-ċiberkriminalità, jistgħu jkunu involuti bosta ġurisdizzjonijiet, li jirrikjedi taħriġ fil-livell tal-UE. U madankollu, is-CEPOL, l-aġenzija tal-UE għat-taħriġ fl-infurzar tal-liġi, osservat li aktar minn żewġ terzi tal-Istati Membri ma jipprovdux taħriġ ċibernetiku regolari lill-uffiċjali tal-infurzar tal-liġi[121]. L-UE tista' wkoll potenzjalment tidentifika modi biex toħloq sinerġiji tal-edukazzjoni u t-taħriġ bejn l-isferi ċivili u militari[122]. Minkejja dan, l-ENISA sabet li filwaqt li l-opportunitajiet attwali ta' taħriġ f'setturi kritiċi huma estensivi, huma ma jimmirawx b'mod suffiċjenti r-reżiljenza tal-infrastruttura kritika[123].

Tabella 2 – Xi wħud mill-inizjattivi ta’ taħriġ relatat mal-qasam ċibernetiku fl-UE

Proġetti tal-Aġenzija Ewropea għad-Difiża, eż. appoġġ relatat mal-eżerċizzji mis-settur privat u l-proġett dwar iċ-Ċiberspazji ta' Taħriġ	Netwerk tal-Kulleġġ Ewropew ta' Sigurtà u ta' Difiża (jipprovdi taħriġ ċivili-militari), inkluża l-Pjattaforma għall-Edukazzjoni, it-Taħriġ, l-Evalwazzjoni u l-Eżerċizzju fil-qasam taċ-Ċibersigurtà	Taħriġ tal-ENISA, li joffri programmi ta' taħriġ fejn is-suq kummerċjali jista’ jonqos milli jipprovdihom
Programmi ta’ taħriġ tal-Europol, is-CEPOL, l-ECTEG[124] – inkluż il-Mudell ta’ Governanza tat-Taħriġ u l-Qafas ta’ Kompetenza fit-Taħriġ (inkluża ċ-ċertifikazzjoni)	Netwerk ta’ Ċentri ta’ Kompetenza u Ċentru ta’ Kompetenza tar-Riċerka (proposti)	Miżuri dwar il-kriptaġġ propost fil-Ħdax-il Rapport ta' Progress tal-Unjoni tas-Sigurtà
Kooperazzjoni bejn l-UE u n-NATO dwar it-taħriġ u l-edukazzjoni fil-qasam taċ-ċiberdifiża	Programm Militari Erasmus	Netwerk Ewropew tat-Taħriġ Ġudizzjarju

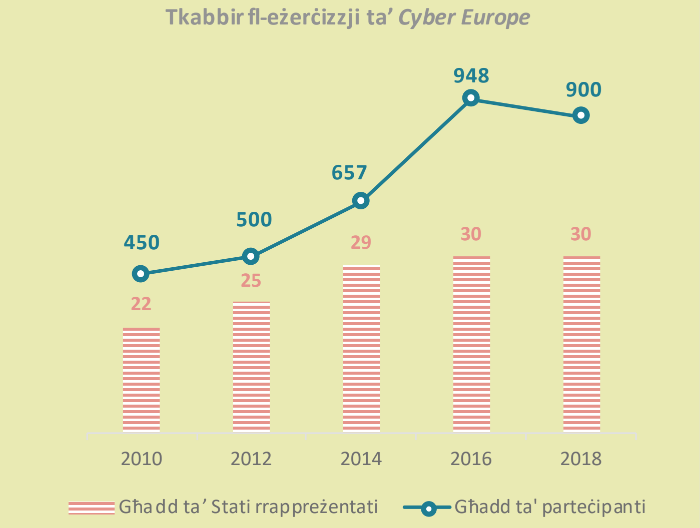
Sors: Il-QEA.

87 L-UE inkarigat esperti tas-sigurtà u tal-ġlieda kontra t-terroriżmu għal 17-il delegazzjoni biex tirrinforza r-rabta bejn is-sigurtà interna u esterna tal-UE[125]. Minkejja l-limitazzjonijiet fir-riżorsi, għarfien espert akbar fil-qasam ċibernetiku jista’ jikkontribwixxi għall-istabbiliment tal-proġetti t-tajbin, kif ukoll għall-identifikazzjoni ta’ sinerġiji ma’ programmi jew sorsi oħra ta’ finanzjament[126]. Huwa jista’ wkoll isaħħaħ il-profil taċ-ċibersigurtà fid-djalogu politiku, għalkemm ikollu jikkompeti ma’ ħafna prijoritajiet oħra, bħall-migrazzjoni, il-kriminalità organizzata jew il-ġellieda barranin li jirritornaw.

Kaxxa 4

Eżerċizzji

L-eżerċizzji huma element importanti tal-edukazzjoni u t-taħriġ fil-qasam taċ-ċibersigurtà, li joffru opportunitajiet primarji biex tingħata spinta lit-tħejjija billi jittestjaw il-kapaċitajiet, joffru rispons għal xenarji reali u jibnu netwerks ta' relazzjonijiet ta' xogħol. Mill-2010 'l hawn, il-frekwenza tagħhom żdiedet b'mod konsiderevoli.



Sors: Il-QEA, ibbażat fuq dokumenti tal-ENISA.

Il-parteċipanti jieħdu sehem fuq il-post jew mill-bogħod. Hemm valutazzjonijiet ta' wara l-eżerċizzji biex jiġu identifikati t-tagħlimiet meħuda, għalkemm dawn jistgħu jkunu għadhom mhux qed jgħaddu għalkollox minn bejn is-saffi strateġiċi/politiċi, operazzjonali u tekniċi[127].

L-eżerċizzji emblematiċi tal-UE u n-NATO – dak biennali Cyber Europe (operazzjonali) u dak annwali Locked Shields (tekniku) – jiġbru aktar minn 1 000 parteċipant minn madwar 30 stat parteċipanti. Iż-żewġ eżerċizzji jiffukaw fuq il-protezzjoni u ż-żamma ta' infrastruttura kritika f'xenarji simulati ta' attakk. L-eżerċizzji saru konsiderevolment aktar approfonditi, u t-tnejn li huma issa jinkludu elementi ta' politika tal-midja, legali u finanzjarja biex jittejjeb l-għarfien tas-sitwazzjoni tal-professjonisti. L-eżerċizzji PACE (strateġiċi) li huma paralleli u kkoordinati jittestjaw l-interazzjoni bejn l-UE u n-NATO f'xenarju ta' kriżi ibrida.

Dawn mhumiex l-uniċi eżerċizzji internazzjonali. L-ENISA torganizza sfida ċibernetika annwali, li fiha t-timijiet jikkompetu biex isolvu l-isfidi relatati mas-sigurtà, bħas-sigurtà tal-web u dik mobbli, taħbil il-moħħ kriptografiku, l-inġinerija inversa, l-etika u l-forensika. L-ewwel eżerċizzju f'livell ministerjali, l-EU CYBRID, seħħ f'Settembru 2017, li kien jiffoka fuq it-teħid ta' deċiżjonijiet strateġiċi. Fl-2018, l-eżerċizzju affiljat man-NATO, Crossed Swords, tnieda biex itejjeb l-elementi offensivi tal-eżerċizzju Locked Shields tagħha. In-NATO torganizza wkoll l-eżerċizzji dwar il-Koalizzjoni Ċibernetika.

Sfida ewlenija hija li jiġu żgurati l-involviment attiv tal-partijiet ikkonċernati kollha u l-koordinazzjoni tal-eżerċizzji kollha, biex tiġi evitata d-duplikazzjoni u t-tagħlimiet meħuda jiġu kondiviżi b'mod effiċjenti.

Sensibilizzazzjoni

88 Iċ-ċittadini huma spiss vetturi għall-attakki u jxerrdu diżinformazzjoni, peress li huma għandhom il-probabbiltà li jkunu esposti inkonxjament għal vulnerabbiltajiet f'apparat u software irħis u distribwit b'mod estensiv jew li jisfaw vittmi tas-social engineering. Iż-żieda tas-sensibilizzazzjoni hija għalhekk essenzjali għall-bini ta' reżiljenza ċibernetika effettiva, madankollu bl-ebda mod ma hija kompitu faċli peress li huwa diffiċli għal persuni mhux esperti li jifhmu l-kumplessità taċ-ċibersigurtà u r-riskji assoċjati.

89 Ix-Xahar iddedikat għaċ-Ċibersigurtà Ewropea (ECSM) u l-Jum għal Internet Aktar Sikur ta' kull sena huma eżempji ta' żieda tas-sensibilizzazzjoni. Issa hemm 7 Stati Membri tal-UE li ngħaqdu mal-ECSM[128]. Il-kampanja *Say No!* tal-Europol għandha l-għan li tnaqqas ir-riskju li tfal jisfaw vittmi tal-koerċizzjoni u estorsjoni sesswali online. It-tnaqqis tar-riskju huwa importanti minħabba li bħalissa, ftit vittmi tal-attakki jirrappurtaw dawn il-każijiet ta' kriminalità lill-pulizija[129]. Il-Kummissjoni tirrikonoxxi li l-istrateġija għaċ-ċibersigurtà kienet biss "parzjalment effettiva" fiż-żieda tas-sensibilizzazzjoni taċ-ċittadini u n-negozji[130]. Dan huwa dovut għall-iskala tal-kompitu, ir-riżorsi limitati, l-involviment mhux uniformi tal-Istati Membri, u nuqqas ta' evidenza xjentifika dwar l-aħjar mod kif tiżdied is-sensibilizzazzjoni u kif din għandha titkejjel.

90 L-isfida għall-Kummissjoni u l-aġenziji rilevanti hija li jiżguraw li l-miżuri ta' żieda tas-sensibilizzazzjoni jkunu: immirati u ppubbliċizzati tajjeb; inklużivi; isegwu x-xenarju tat-theddid; jevitaw effetti mhux intenzjonati bħall-"eżawriment minħabba s-sigurtà"[131]; u jiżviluppaw metodi ta' evalwazzjoni u metrika biex jivvalutaw l-effettività tagħhom. Dan għandu japplika b'mod ugwali fi ħdan l-istituzzjonijiet tal-UE nfushom, fejn il-kultura ta' sensibilizzazzjoni teħtieġ titjib[132].

Sfida 8: skambju ta' informazzjoni u koordinazzjoni aħjar

91 Iċ-ċibersigurtà tirrikjedi kooperazzjoni bejn is-settur pubbliku u dak privat, primarjament f'termini ta' kondiviżjoni tal-informazzjoni u ta' skambju tal-aħjar prattiki. Il-fiduċja hija essenzjali fil-livelli kollha biex jinħoloq l-ambjent it-tajjeb għall-kondiviżjoni tal-informazzjoni sensittiva lil hinn mill-fruntieri. Koordinazzjoni fqira twassal għal frammentazzjoni, duplikazzjoni tal-isforzi u tixrid ta' għarfien espert. Koordinazzjoni effettiva tista' tirriżulta f'suċċessi tanġibbli, bħall-għeluq ta' swieq tad-darkweb[133]. Minkejja l-progress miksub fi snin reċenti, il-livelli ta' fiduċja għadhom "insuffiċjenti"[134] fil-livell tal-UE u f'xi wħud mill-Istati Membri[135].

Koordinazzjoni fost l-istituzzjonijiet tal-UE u mal-Istati Membri

92 Wieħed mill-għanijiet tal-Istrateġija għaċ-Ċibersigurtà, u tal-istrutturi kooperattivi introdotti mid-Direttiva NIS, kien li jsaħħaħ il-fiduċja fost il-partijiet ikkonċernati. Il-valutazzjoni tal-istrateġija rrikonoxxiet li kien ġie stabbilit pedament għall-kooperazzjoni strateġika u operazzjonali fil-livell tal-UE[136]. Minkejja dan, il-koordinazzjoni inġenerali hija "insuffiċjenti"[137]. L-isfida hija li jiġi żgurat li l-iskambju ta' informazzjoni mhux biss ikun siewi iżda jkun jippermetti wkoll stampa ġenerali kompleta tal-perspettiva ġenerali. L-ilħuq ta' fehim komuni bbażat fuq terminoloġija aċċettata huwa fattur importanti f'dan ir-rigward (ara l-***Kaxxa 5***).

93 L-evalwazzjoni tal-EBISA osservat, madankollu, li l-approċċ tal-UE għaċ-ċibersigurtà ma kienx ikkoordinat biżżejjed, u dan irriżulta f'nuqqas ta' sinerġiji bejn l-attivitajiet tal-ENISA u dawk ta' partijiet ikkonċernati oħra. Il-mekkaniżmi ta' kooperazzjoni għadhom relattivament immaturi[138]; l-Att dwar iċ-Ċibersigurtà biħsiebu jindirizza dan billi jsaħħaħ ir-rwol ta' koordinazzjoni tal-ENISA. Din ix-xewqa li tissaħħaħ il-kooperazzjoni kienet ir-raġunament wara l-memorandum ta' qbil li ġie ffirmat fl-2018 bejn l-ENISA, l-EDA, l-EC3 tal-Europol, u s-CERT-UE[139]. Prijorità għall-Kummissjoni fis-snin li ġejjin se tkun li jiġi żgurat allinjament xieraq bejn l-inizjattivi ta' politika, il-ħtiġijiet u l-programmi ta' investiment sabiex tingħeleb il-frammentazzjoni u jiġu ġġenerati sinerġiji[140].

94 Il-funzjonijiet ta' koordinazzjoni huma inkorporati fi ħdan diversi korpi istituzzjonali. It-Task Force dwar l-Unjoni tas-Sigurtà ġiet stabbilita biex ikollha rwol ċentrali fil-koordinazzjoni tad-direttorati Ġenerali differenti tal-Kummissjoni bil-ħsieb li tappoġġa l-aġenda tal-Unjoni tas-Sigurtà[141]. Id-DĠ CNECT jippresiedi s-sottogrupp ta' ħidma tat-Task Force dwar iċ-ċibersigurtà.

95 Fil-Kunsill, iċ-ċibersigurtà hija ttrattata mill-Grupp ta' Ħidma Orizzontali dwar Kwistjonijiet ta' Ċiberspazju (HWP), li jikkoordina kwistjonijiet strateġiċi u orizzontali ta' ċiberspazju, kif ukoll jgħin fit-tħejjija tal-eżerċizzji u jevalwa r-riżultati tagħhom. Huwa jaħdem mill-qrib mal-Kumitat Politiku u ta' Sigurtà, li għandu rwol ċentrali ta' teħid ta' deċiżjonijiet fir-rigward ta' kwalunkwe miżura diplomatika relatata mal-qasam ċibernetiku (ara l-***Kaxxa 6*** fil-kapitolu li jmiss). Peress li ċ-ċibersigurtà hija suġġett trażversali, il-koordinazzjoni tal-interessi rilevanti kollha mhix sempliċi: mhux inqas minn 24 grupp ta' ħidma u korpi preparatorji dan l-aħħar ittrattaw kwistjonijiet relatati mal-qasam ċibernetiku[142].

96 Iż-żewġ proposti leġiżlattivi l-aktar reċenti dwar it-tisħiħ tal-ENISA (2017) u dwar l-istabbiliment ta' netwerk ta' ċentri ta' kompetenza dwar iċ-ċibersigurtà u ta' ċentru ta'

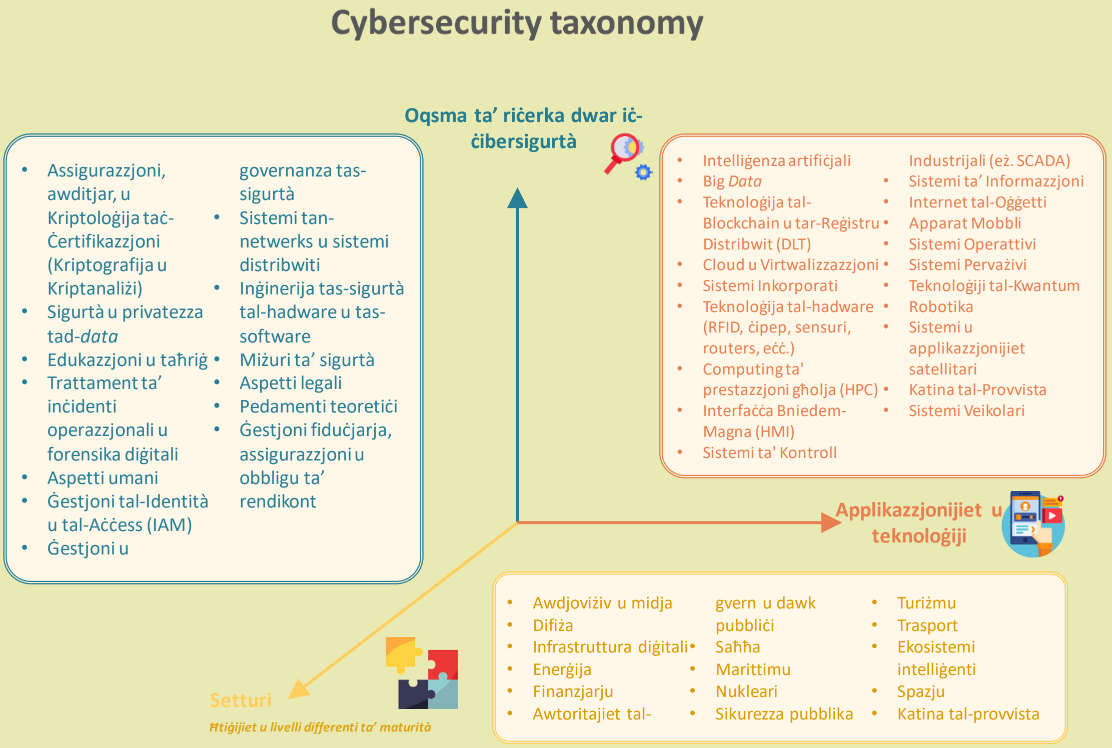
kompetenza tar-riċerka (2018) huma speċifikament maħsuba biex jindirizzaw il-frammentazzjoni u d-duplikazzjoni tal-isforzi. Fattur ewlieni wara n-netwerk ta’ ċentri ta’ kompetenza dwar iċ-ċibersigurtà u ta’ ċentru ta’ kompetenza tar-riċerka kien il-ħtieġa li titneħħa d-diskrepanza li l-istrutturi kooperattivi tad-Direttiva NIS ma jneħħux, peress li ma kinux maħsuba biex jappoġġaw l-iżvilupp ta’ soluzzjonijiet “mill-aktar avvanzati”.

Kaxxa 5

Nippruvaw nitkellmu l-istess lingwa ċibernetika: *koerenza teknoloġika*

Iċ-ċarezza terminoloġika ttejjeb l-għarfien tas-sitwazzjoni u l-koordinazzjoni[143] u tikkontribwixxi għall-istabbiliment preċiż ta’ dak li jikkostitwixxi theddida jew riskju.

Iċ-Ċentru Konġunt tar-Riċerka (JRC) tal-Kummissjoni dan l-aħħar żviluppa tassonomija riveduta ta’ riċerka meħuda minn standards internazzjonali differenti[144]. L-għanijiet tagħha huma li ssir punt ta’ referenza biex tintuża bħala indiċi mill-entitajiet ta' riċerka fl-Ewropa kollha.



Sors: Il-QEA, adattat mill-Kummissjoni Ewropea.

Sa ftit ilu, l-istituzzjonijiet u l-aġenziji tal-UE ma kellhomx definizzjonijiet komuni. Dan qed jinbidel. Fil-qafas tal-pjan ta’ azzjoni tiegħu, il-Grupp ta' Kooperazzjoni fassal tassonomija ta’ inċidenti bl-għan li jiffaċilita kollaborazzjoni transkonfinali effiċjenti.

Kooperazzjoni u skambju ta' informazzjoni mas-settur privat

97 Il-kooperazzjoni bejn l-awtoritajiet pubbliċi u s-settur privat hija essenzjali għat-tisħiħ tal-livelli kumplessivi ta' ċibersigurtà. Minkejja dan, fil-valutazzjoni li hija wettqet fl-2017 tal-Istrateġija għaċ-Ċibersigurtà, il-Kummissjoni sabet li l-iskambju ta' informazzjoni fost il-partijiet ikkonċernati privati u bejn is-settur pubbliku u dak privat kien għadu mhuwiex ottimu minħabba nuqqas ta' mekkaniżmi ta' rappurtar u inċentivi fdati għall-kondiviżjoni ta' informazzjoni[145], li xekkel l-ilħuq ta' għanijiet strateġiċi. Il-Kummissjoni osservat ukoll in-nuqqas ta' mekkaniżmu ta' kooperazzjoni effiċjenti li permezz tiegħu l-Istati Membri jaħdmu flimkien biex isaħħu b'mod strateġiku l-kapaċitajiet industrijali dejjiema f'dan il-livell[146].

98 Iċ-Ċentri tal-Kondiviżjoni u tal-Analiżi tal-Informazzjoni (ISACs) huma organizzazzjonijiet stabbiliti biex jipprovdu pjattaformi u riżorsi biex jiffaċilitaw il-kondiviżjoni tal-informazzjoni bejn is-settur pubbliku u dak privat kif ukoll biex jiġbru informazzjoni dwar it-theddid ċibernetiku. Huma għandhom l-għan li jibnu l-fiduċja permezz ta' kondiviżjoni ta' esperjenzi, għarfien u analiżi, speċjalment dwar il-kawżi ewlenin, l-inċidenti u t-theddid. Diġà jeżistu ISACs nazzjonali u settorjali f'ħafna Stati Membri, iżda fil-livell Ewropew, dawn għadhom relattivament limitati[147]. Madankollu, dawn jiġu ma' għadd ta' sfidi (limitazzjonijiet fil-forniment ta' riżorsi, diffikultajiet fl-evalwazzjoni tas-suċċess tagħhom, l-iżgurar tal-istrutturi t-tajbin biex ikun involut kemm is-settur pubbliku kif ukoll dak privat, l-involviment tal-awtoritajiet tal-infurzar tal-liġi) li jkun jeħtieġ li jingħelbu sabiex jikkontribwixxu għall-implimentazzjoni tad-Direttiva NIS u għat-tisħiħ tal-kapaċitajiet ta' sigurtà fl-Ewropa kollha[148].

99 Kooperazzjoni mill-qrib mas-settur privat hija partikolarment importanti għall-ġlieda kontra ċ-ċiberkriminalità kumplessa, iżda l-effiċjenza tagħha mhix uniformi fl-Istati Membri u tiddependi mil-livell ta' fiduċja[149]. L-EC3 tal-Europol, madankollu, stabbilixxa sensiela ta' gruppi konsultattivi mal-operaturi tas-settur privat, l-istituzzjonijiet u l-aġenziji tal-UE, kif ukoll organizzazzjonijiet internazzjonali oħra biex itejjeb il-kollaborazzjoni permezz ta' netwerking, kondiviżjoni strateġika ta' intelligence u kooperazzjoni. Huma jaħdmu skont il-pjanijiet allinjati mal-għanijiet taċ-Ċiklu ta' Politika tal-UE[150]. L-abbuż kriminali tal-kriptaġġ huwa qasam ieħor mimli sfidi li jappellaw għal aktar kooperazzjoni mas-settur privat. Attwalment, l-EC3 tal-Europol qed jeżamina l-possibbiltajiet biex jospita rabtiet fuq terminu qasir speċifiċi għall-każ mal-J-CAT (ara l-paragrafu *62*) għal esperti mis-settur privat u minn istituzzjonijiet akkademiċi.

100 Il-komunitajiet ċivili u ta' difiża – kemm pubbliċi kif ukoll privati – qed ibatu minn nuqqas ta' mekkaniżmi ta' kooperazzjoni effiċjenti. L-oqsma li jippreżentaw sfida

komuni huma l-kriptografija, is-sistemi inkorporati siguri, l-identifikazzjoni ta' malware, it-tekniki ta' simulazzjoni, il-protezzjoni tan-netwerks u tas-sistemi ta' komunikazzjoni u t-teknoloġiji ta' awtentikazzjoni. Il-promozzjoni tal-kooperazzjoni ċivili-militari u l-appoġġ għar-riċerka u t-teknoloġija (b'mod partikolari bl-appoġġ għall-SMEs) huma tnejn mill-prijoritajiet fil-Qafas aġġornat ta' Politika tal-UE dwar iċ-Ċiberdifiża (aġġornament tal-2018).

Punti ta' riflessjoni – Bini tar-reżiljenza

- Kif jista' jinkiseb bilanċ xieraq fil-livell tal-UE bejn il-ħtieġa li tiġi integrata politika fil-qasam taċ-ċibersigurtà u li tiġi żgurata koordinazzjoni effiċjenti bejn id-diversi atturi u t-tixrid ta' responsabbiltajiet?
- L-istituzzjonijiet u l-aġenziji tal-UE kemm huma mħejjija tajjeb għall-attakk il-kbir li jmiss imniedi direttament kontrihom?
- L-aġenziji rilevanti tal-UE għaċ-ċiberspazju kif jistgħu jattiraw aktar talent?
- X'passi ulterjuri huma meħtieġa għall-iżgurara ta' kapaċità adegwata fl-istituzzjonijiet u l-aġenziji kollha tal-UE biex ikun permess qafas koerenti ta' valutazzjoni tar-riskji u tat-theddid?
- B'liema modi l-awtoritajiet superviżorji Ewropej (Awtorità Bankarja Ewropea, l-Awtorità Ewropea tat-Titoli u s-Swieq u l-Awtorità Ewropea tal-Assigurazzjoni u l-Pensjonijiet tax-Xogħol) qed jindirizzaw il-vulnerabbiltajiet ċibernetiċi inerenti fis-settur finanzjarju, u x'tagħlimiet jistgħu jittieħdu minn dan għal setturi oħra?
- Bin-nuqqas kumplessiv fl-għarfien espert, l-assistenza teknika tal-UE għall-awtoritajiet pubbliċi kif tista' tintuża bl-aħjar mod biex ikollha l-impatt kumplessiv massimu fit-titjib tal-reżiljenza ċibernetika?
- L-UE u l-Istati Membri kif jistgħu jiżguraw preżenza siewja fid-diskuzzjonijiet internazzjonali biex jifformulaw il-governanza u l-istandards taċ-ċiberspazju u jippromwovu l-valuri tal-UE?
- Liema miżuri ta' żieda tas-sensibilizzazzjoni fil-livell tal-UE u f'dak tal-Istati Membri (inklużi l-isforzi ta' prevenzjoni) qegħdin verament jagħmlu differenza, u x'tista' tagħmel l-UE biex iżżidhom?
- L-UE xi rwol għandha biex tikkontribwixxi għall-ksib ta' diversità tal-ġeneru fil-qasam taċ-ċibersigurtà?
- L-UE u l-Istati Membri kif jistgħu jsaħħu s-sinerġiji bejn il-komunitajiet ċivili u ta' difiża, f'konformità mal-Qafas ta' Politika dwar iċ-Ċiberdifiża (aġġornament tal-2018)?

Rispons effettiv għal inċidenti ċibernetiċi

101 It-tfassil ta' rispons effettiv għal ċiberattakki huwa fundamentali biex dawn jitwaqqfu fl-insegwimenti tagħhom kmieni kemm jista' jkun. Huwa partikolarment importanti li s-setturi kritiċi, l-Istati Membri u l-istituzzjonijiet tal-UE jkunu jistgħu jirreaġixxu b'mod rapidu u kkoordinat. L-identifikazzjoni bikrija hija essenzjali għal dan.

Sfida 9: identifikazzjoni u rispons effettivi

Identifikazzjoni u notifika

102 L-għodod komuni ta' identifikazzjoni jgħinu biex tingħeleb il-maġġoranza l-kbira ta' attakki fuq bażi ta' kuljum[151]. Minkejja dan, is-sistemi diġitali tant saru kumplessi li huwa impossibbli kull attakk jiġi pprevenut. Is-sofistikazzjoni tagħhom tfisser li l-attakki spiss jevadu l-identifikazzjoni għal perjodi twal. L-esperti jgħidu, għalhekk, li l-fokus għandu jkun fuq l-identifikazzjoni u d-difiża rapidi[152]. Madankollu, xi għodod ta' identifikazzjoni bħall-awtomatizzazzjoni, it-tagħlim awtomatiku u l-analitika tal-imġiba, li għandhom l-għan li jnaqqsu r-riskji, u li janalizzaw u jitgħallmu mill-imġiba tas-sistemi – jippreżentaw rati baxxi ta' adozzjoni min-negozji[153]. Dan huwa parzjalment dovut għall-ġenerazzjoni ta' pożittivi foloz, fejn attivitajiet mhux ta' theddid jiġu ġġudikati ħażin bħala malizzjużi.

103 Ladarba jkun inqabad u ġie analizzat ksur tar-regoli, jinħtieġu notifika u rappurtar rapidi biex b'hekk entitajiet pubbliċi u dawk privati oħra jistgħu jieħdu azzjoni preventiva, u l-awtoritajiet rilevanti jistgħu jappoġġaw dawk li jiġu affettwati. Ħafna organizzazzjonijiet ma għandhomx wisq rieda li jirrikonoxxu u jirrappurtaw inċidenti ċibernetiċi[154]. L-involviment bikri tal-awtoritajiet tal-infurzar tal-liġi fir-rispons inizjali għall-każijiet ta' ċiberkriminalità suspettata u l-iskambju ta' informazzjoni proattiva mas-CSIRTs huwa wkoll essenzjali.

104 In-nuqqas preċedenti ta' rekwiżiti komuni tal-UE dwar in-notifika ta' inċidenti kellu r-riskju li jdewwem il-komunikazzjoni tal-każijiet ta' ksur tar-regoli u jxekkel ir-rispons, li l-introduzzjoni tad-Direttiva NIS kellha l-għan li tindirizza (ara l-paragrafu ***20***). Wara l-attakki minn *Wannacry* li seħħew fl-2017, il-Kummissjoni kkonkludiet li s-sistema tan-netwerk tas-CSIRTs kienet għadha mhix kompletament operazzjonali[155]. Hekk kif l-implimentazzjoni tad-Direttiva tkompli, għad irid jiġi stabbilit jekk il-gwida

żviluppata mill-Grupp ta' Kooperazzjoni hijiex se tkun effettiva biex jingħeleb in-nuqqas ta’ rieda li l-inċidenti jiġu rrappurtati[156].

105 L-operaturi ta’ servizzi essenzjali f’ċerti setturi għandhom bosta obbligi ta' notifika (inkluż lill-konsumaturi) skont regolamenti eżistenti tal-UE, li jistgħu jxekklu l-effiċjenza tal-proċess. Pereżempju, l-operaturi fis-settur bankarju u f’dak finanzjarju huma suġġetti għal kriterji ta’ notifika, standards, sollijiet u limiti ta’ żmien skont il-GDPR, id-Direttiva NIS, id-Direttiva dwar is-Servizzi ta' Ħlas, il-BĊE/l-MSU, Target 2 u r-Regolament eIDAS[157]. Għalhekk, huwa importanti li dawn l-obbligi jiġu ssimplifikati peress li, minbarra li tikkostitwixxi piż amministrattiv bla bżonn, din l-eteroġeneità tista’ twassal għal rappurtar frammentat.

Rispons ikkoordinat

106 L-iżvilupp ta’ qafas ta' kooperazzjoni Ewropea fi kriżijiet ta' ċibersigurtà għadu xogħol fl-idejn. Il-“pjan ta’ azzjoni”[158] relatat (ara l-paragrafu *18*) ġie għalhekk introdott biex jintroduċi perspettiva ċibernetika fil-mekkaniżmu ta’ Rispons Politiku Integrat f'Sitwazzjonijiet ta' Kriżi (IPCR), itejjeb l-għarfien tas-sitwazzjoni u jiżgura integrazzjoni aħjar ma’ mekkaniżmi oħra ta’ ġestjoni ta' kriżijiet tal-UE[159]. Huwa jinvolvi l-istituzzjonijiet, l-aġenziji u l-Istati Membri tal-UE. L-integrazzjoni mingħajr xkiel ta’ dawn il-mekkaniżmi kollha ta’ rispons għall-kriżijiet hija problematika[160]. In-nuqqas attwali ta’ netwerk konġunt u sigur ta’ komunikazzjoni fl-istituzzjonijiet tal-UE huwa wkoll nuqqas importanti[161].

107 Il-kapaċità tal-UE li tirreaġixxi għal ċiberattakki fil-livell operazzjonali u f’dak politiku f’każ ta’ inċident transkonfinali ta’ skala kbira ġiet ikklassifikata bħala “limitata”, parzjalment minħabba li ċ-ċibersigurtà għadha mhix integrata f’mekkaniżmi ta' koordinazzjoni eżistenti tar-rispons għall-kriżijiet fil-livell tal-UE[162]. Dan mhuwiex indirizzat fid-Direttiva NIS.

108 Ir-riforma tal-ENISA li ġiet proposta dan l-aħħar, u li kienet tipprevedi rwol operazzjonali akbar fit-trattament ta’ inċidenti fuq skala kbira relatati maċ-ċibersigurtà, ma kinitx appoġġata mill-Istati Membri, billi kienu jippreferu li r-rwol tal-aġenzija jkun jappoġġa u jikkomplementa l-azzjoni operazzjonali proprja tagħhom[163]. Diġà hemm ħafna CERTs/CSIRTs fil-livell tal-Istati Membri, iżda l-kapaċitajiet tagħhom ivarjaw b’mod konsiderevoli. Dan jikkostitwixxi ostaklu għall-kooperazzjoni transkonfinali effettiva meħtieġa għar-rispons għal inċidenti ta’ skala kbira[164].

109 Aħna ppruvajna nimmappjaw ir-rwoli differenti assenjati għall-atturi differenti fil-pjan ta' azzjoni, iżda kien hemm xi lakuni li se jkun jeħtieġ li jimtlew hekk kif l-implimentazzjoni tavvanza. Qasam partikolari li inizjalment ma ġiex indirizzat b'mod suffiċjenti kien l-infurzar tal-liġi, għalkemm il-Protokoll ta' Rispons ta' Emerġenza għall-Infurzar tal-Liġi tal-UE daħal fis-seħħ f'Diċembru 2018[165]. L-iżgurar li l-pjan ta' azzjoni huwa prattiku u li l-partijiet kollha jafu x'għandhom jagħmlu huwa essenzjali għas-suċċess tiegħu; dan se jkun jeħtieġ ittestjar estensiv fis-snin li ġejjin.

110 Ir-rispons effettiv mhuwiex biss il-limitazzjoni tal-ħsara; l-assenzjazzjoni tar-responsabbiltà għall-attakki hija wkoll kruċjali. L-insegwiment u l-identifikazzjoni tal-awturi, fuq kollox f'attakk ibridu, jistgħu jkunu diffiċli minħabba l-abbuż dejjem akbar tal-għodod ta' anonomizzazzjoni, il-kriptovaluti u l-kriptaġġ. Dan huwa magħruf bħala l-problema tal-attribuzzjoni. Ir-rimedju ta' din il-problema mhuwiex biss kwistjoni teknika; huwa wkoll sfida ta' ġustizzja kriminali. Id-differenzi legali u proċedurali bejn il-pajjiżi jistgħu jimpedixxu l-investigazzjonijiet kriminali u l-prosekuzzjoni ta' persuni ssuspettati. L-indirizzar tal-problema tal-attribuzzjoni se tkun teħtieġ skambju ta' informazzjoni operazzjonali aktar formalizzat permezz ta', pereżempju, proċeduri aktar ċari mal-Europol jew in-Netwerk Ġudizzjarju Ewropew kontra ċ-Ċiberkriminalità tal-Eurojust.

111 Fil-livell politiku, is-sett ta' għodod taċ-ċiberdiplomazija (ara l-*Kaxxa 6*) ġie żviluppat sabiex jappoġġa s-soluzzjoni ta' tilwim internazzjonali fiċ-ċiberspazju b'mezzi paċifiċi. Il-ħolqien ta' timijiet ta' rispons rapidu ċibernetiku u ta' inizjattiva għal assistenza reċiproka fil-qasam taċ-ċibersigurtà huma żewġ proġetti li jrawmu l-kondiviżjoni mtejba tal-informazzjoni u li qed jiġu żviluppati taħt il-qafas tal-PESCO[166].

Kaxxa 6

Is-sett ta' għodod taċ-ċiberdiplomazija

Ir-Rispons Diplomatiku Konġunt tal-UE għal Attivitajiet Ċibernetiċi Malizzjużi [167], jew is-"sett ta' għodod taċ-ċiberdiplomazija", li oriġinaw mill-Konklużjonijiet tal-Kunsill dwar iċ-Ċiberdiplomazija tal-2015[168]. Iċ-ċiberdiplomazija għandha l-għan li tiżviluppa u timplimenta approċċ komuni u komprensiv għaċ-ċiberspazju bbażat fuq il-valuri tal-UE, l-istat tad-dritt, it-tisħiħ tal-kapaċitajiet u s-sħubiji, il-promozzjoni tal-mudell b'bosta partijiet ikkonċernati tal-governanza tal-internet, kif ukoll il-mitigazzjoni tat-theddid ċibernetiku u l-istabbiltà akbar fir-relazzjonijiet internazzjonali.

Is-sett ta' għodod jippermetti lill-UE u lill-Istati Membri tagħha li jifformulaw rispons diplomatiku konġunt għal attivitajiet ċibernetiċi malizzjużi billi jagħmlu użu sħiħ minn miżuri fi ħdan il-Politika Estera u ta' Sigurtà Komuni. Dawn jistgħu jinkludu miżuri preventivi (eż. żieda tas-sensibilizzazzjoni, tisħiħ tal-kapaċitajiet), kooperattivi, miżuri

ta' stabbiltà u restrittivi (eż. projbizzjonijiet fuq l-ivvjaġġar, embargi fuq l-armi, iffriżar ta' fondi) jew appoġġ għar-rispons tal-Istati Membri[169]. L-idea hija li aktar kooperazzjoni għall-mitigazzjoni tat-theddid u s-sinjalar ċar tal-konsegwenzi probabbli ta' rispons konġunt jistgħu (potenzjalment) jiskoraġġixxu imġiba aggressiva.

Rispons konġunt tal-UE għal attivitajiet ċibernetiċi malizzjużi jkun proporzjonat għall-ambitu, l-iskala, id-durata, l-intensità, il-kumplessità, is-sofistikazzjoni u l-impatt tal-attività ċibernetika.

Parti integrali tas-suċċess tas-sett ta' għodod tkun kemm dan huwa minsuġ tajjeb mal-pjan ta' azzjoni u l-IPCR (ara l-paragrafu ***106***), kemm l-għarfien tas-sitwazzjoni huwa stabbilit tajjeb permezz tal-kondiviżjoni rapida u kontinwa tal-informazzjoni (inkluża dik dwar l-elementi ta' attribuzzjoni)[170] u, fl-aħħar nett, il-kooperazzjoni effettiva. Barra minn hekk, komunikazzjoni effettiva u kkoordinata hija wkoll essenzjali għall-użu b'suċċess tas-sett ta' għodod. Sa issa, is-sett ta' għodod intuża darbtejn: biex jinbeda djalogu mal-Istati Uniti wara l-attakk minn *Wannacry*[171], u biex jiġu żviluppati l-konklużjonijiet tal-Kunsill li jikkundannaw l-użu malizzjuż tal-ICT[172]. L-operazzjonalizzazzjoni tas-sett ta' għodod għadha għaddejja; għad irid jiġi stabbilit kemm dan se jkun effettiv fl-ilħuq tal-objettivi tiegħu.

Sfida 10: protezzjoni tal-infrastruttura kritika u l-funzjonijiet tas-soċjetà

Protezzjoni tal-infrastruttura

112 Il-biċċa l-kbra mill-infrastruttura kritika tal-UE hija operata permezz ta' sistemi ta' kontroll industrijali (ICS)[173]. Ħafna minn dawn tfasslu bħala sistemi indipendenti, b'konnettività limitata għad-dinja esterna. Billi komponenti tal-ICS ġew konnessi mal-internet, huma saru aktar vulnerabbli għal interferenza esterna. Iż-żamma ta' sistemi eżistenti u l-użu ta' software korrettiv għalihom jistgħu ma jibqgħux possibbli, iżda l-aġġornament tagħhom ma jinkisibx malajr u mhuwiex irħis. L-isforzi għat-tisħiħ tas-sigurtà ta' infrastruttura kritika jridu għalhekk jinkludu l-aġġornament tal-ICS.

113 Hekk kif l-industrija tkompli tiġi diġitalizzata (komunement magħrufa bħala "Industrija 4.0"), l-impatt ta' inċident fuq skala kbira f'settur industrijali jista' jkollu effett negattiv bnadi oħra. L-ENISA osservat l-importanza tal-immappjar tal-impatt ta' dipendenzi reċiproċi tas-setturi kritiċi[174]. Dan huwa essenzjali għall-fehim tat-tixrid potenzjali ta' inċident u huwa bbażat fuq rispons ikkoordinat sew.

114 Id-Direttiva NIS għandha l-għan li ssaħħaħ il-livell ta' tħejjija f'setturi ewlenin li huma responsabbli għall-infrastruttura kritika. Madankollu, mhux is-setturi kollha huma koperti (ara t-***Tabella 1***)[175], li jnaqqas l-effettività tal-istrateġija[176]: tħassib partikolari f'dan ir-rigward huwa l-protezzjoni tal-integrità demokratika tal-elezzjonijiet minn interferenza fl-infrastruttura elettorali u d-diżinformazjoni (ara l-***Kaxxa 7***). Minbarra r-reviżjoni ta' leġiżlazzjoni eżistenti, għalhekk, sfida ewlenija tkun li wieħed jara l-mod kif dawn is-setturi għandhom jiġu involuti f'rispons effettiv għal inċidenti fuq skala kbira.

115 Il-vulnerabbiltajiet fl-infrastruttura kritika ma jiqfux fil-fruntieri tal-Ewropa. Sfida partikolari għall-kummissjoni hija li tħeġġeġ lil pajjiżi kandidati biex jadottaw l-istess standards bħall-Istati Membri, pereżempju f'oqsma bħal-leġiżlazzjoni relatata mal-qasam ċibernetiku jew il-protezzjoni tal-infrastruttura kritika.

Kaxxa 7

Protezzjoni tal-funzjonijiet kritiċi tas-soċjetà: *il-ġlieda kontra l-interferenza elettorali*

F'Mejju 2019, madwar 400 miljun votant se jivvutaw fl-elezzjonijiet parlamentari Ewropej, l-ewwel li se jsiru skont il-GDPR. Dawn jiġu b'segwitu għal skandli li jikkonċernaw l-abbuż ta' *data* personali għall-mikroimmirar politiku u l-kampanji kkoordinati ta' diżinformazzjoni mingħajr preċedent ("Fake News"). Il-Kummissjoni wissiet dwar il-probabbiltà ta' interferenza fil-qasam ċibernetiku f'dawn l-elezzjonijiet[177]; il-ġlieda kontra din se tkun tirrikjedi approċċ globali minn kull livell tal-gvern u minn kull livell tas-soċjetà.

Infrastruttura elettorali

L-organizzazzjoni tal-elezzjonijiet hija kumplessa, u l-iżgurar tal-protezzjoni u l-integrità tagħhom hija r-responsabbiltà tal-Istati Membri. L-interferenza fl-elezzjonijiet u fl-infrastruttura elettorali jista' jkollha l-għan li tinfluwenza l-preferenzi tal-votanti, il-parteċipazzjoni tal-votanti jew fil-proċess tal-elezzjoni nnifsu, inkluża l-votazzjoni nfisha, kif ukoll it-tabulazzjoni tal-voti u l-komunikazzjoni. Fl-elezzjonijiet għall-Parlament Ewropew, il-protezzjoni tal-hekk imsejjaħ l-"aħħar mil" (il-komunikazzjoni tar-riżultati mill-kapitali nazzjonali għal Brussell) hija partikolarment sfida kritika, minħabba li l-ebda approċċ komuni fil-qasam tas-sigurtà ma jeżisti jew ma ġie ttestjat għal dan[178].

Il-pakkett tal-elezzjoni reċenti tal-Kummissjoni kien jinkludi miżuri għat-tisħiħ taċ-ċibersigurtà elettorali, bħall-ħatra ta' punti ta' kuntatt nazzjonali biex jikkoordinaw u jiskambjaw informazzjoni fit-tħejjija ta' qabel l-elezzjoni. Il-kondiviżjoni tal-aħjar prattiki u t-tagħlimiet meħuda huma ta' importanza partikolari[179].

Is-sistemi elettorali ma jitqisux bħala parti minn infrastruttura kritika[180], lanqas ma huma koperti mid-Direttiva NIS. Minkejja dan, il-Grupp ta' Kooperazzjoni żviluppa gwida prattika dwar is-sigurtà tat-teknoloġija elettorali biex jagħti appoġġ lil awtoritajiet pubbliċi. Il-punti ta’ kuntatt nazzjonali huma mistennija li jiltaqgħu fil-bidu tal-2019[181]. L-Istati Membri huma wkoll imħeġġa jwettqu valutazzjonijiet tar-riskji dwar it-theddid ċibernetiku għall-proċessi elettorali tagħhom.

Diżinformazzjoni

Id-diżinformazzjoni hija element dejjem aktar importanti tal-attakki ibridi li jinvolvi ċiberattakki u l-hacking ta’ netwerks. Dawn jistgħu jintużaw biex jaqsmu s-soċjetajiet, jiżirgħu n-nuqqas ta' fiduċja u jdgħajfu l-fiduċja fi proċessi demokratiċi jew kwistjonijiet oħra (pereżempju, l-aġenda kontra t-tilqim jew it-tibdil fil-klima). Hija kibret fl-iskala, fil-veloċità u fil-firxa, kif ukoll tippreżenta theddida ġenwina għas-sigurtà tal-UE.

L-UE ħadet għadd ta’ miżuri biex tindirizza d-diżinformazzjoni. Mill-2015 'il quddiem, it-Task Force East StratCom ibbażata fis-SEAE ġiet stabbilita biex jiġu kkontestati l-kampanji ta' diżinformazzjoni Russi[182]. Esperti faħħru l-ħidma tagħha fil-promozzjoni ta’ politiki tal-UE, filwaqt li appoġġaw il-midja indipendenti fil-Viċinat, u pprevedew, segwew u indirizzaw id-diżinformazzjoni[183]. Madankollu, ir-riżorsi tat-Task Force huma limitati meta mqabbla mal-iskala u l-kumplessità tal-kampanji ta’ diżinformazzjoni[184]. Jinħtieġu interazzjoni aktar sistematika ma’ strutturi eżistenti tal-UE u kooperazzjoni mtejba tal-komunikazzjoni strateġika[185]. Pjan ta' azzjoni ġdid[186] ġie approvat mill-Kunsill Ewropew f’Diċembru 2018.

Aktar reċentement, il-Kummissjoni, fuq il-bażi tal-Komunikazzjoni tagħha ta’ April 2018 dwar l-indirizzar tad-diżinformazzjoni online[187], żviluppat kodiċi ta’ prattika awtoregolatorju u volontarju[188], li huwa bbażat fuq strumenti ta' politika eżistenti li għalihom iffirmaw il-pjattaformi online u l-industrija tar-reklamar[189]. L-azzjoni tinkludi l-kontribut għaż-żieda fl-affidabbiltà tal-kontenut u l-appoġġ għall-isforzi biex jiżdied il-litteriżmu medjatiku u tal-aħbarijiet. Tnieda wkoll netwerk Ewropew indipendenti ta’ verifikaturi tal-fatti.

Il-Kummissjoni ddikjarat li jistgħu jsegwu miżuri regolatorji oħra jekk il-kodiċi ta’ prattika ma jiġix osservat. Id-determinazzjoni tal-effettività tal-miżuri se tkun kruċjali, b’mod partikolari fid-deċiżjoni dwar kif għandu jitkejjel it-titjib fil-fiduċja, fit-trasparenza u fl-obbligu ta’ rendikont.

Sfida oħra se tkun li jinstabu modi kif jittejbu l-identifikazzjoni, l-analiżi u l-esponiment ta’ diżinformazzjoni[190]. Jinħtieġu wkoll il-monitoraġġ u l-analiżi attivi u strateġiċi ta’ sorsi miftuħa tad-*data*[191]. Tentattivi biex jinkiseb fehim aħjar tal-ambjent ta’ theddid għandhom ikopru wkoll xejriet emerġenti, bħal “deepfakes” (vidjos foloz li jkunu saru bl-għajnuna ta’ intelliġenza artifiċjali u tagħlim awtomatiku approfondit), kif ukoll l-għodod meħtieġa biex jidentifikawhom.

Tisħiħ tal-awtonomija

116 L-UE hija importatur nett ta' prodotti u servizzi taċ-ċibersigurtà, li jżid ir-riskju tad-dipendenza teknoloġika fuq l-operaturi mhux tal-UE, u l-vulnerabbiltà għalihom[192]. B'mod partikolari, din ir-realtà ddgħajjef is-sigurtà tal-infrastruttura kritika tal-UE, li hija appoġġata wkoll mill-ktajjen tal-provvista globali u kumplessi. Ir-riskju jkompli jiġi aggravat fejn l-operaturi mhux tal-UE jakkwistaw ditti taċ-ċibersigurtà Ewropej. L-Istati Membri huma responsabbli għall-iskrinjar tal-Investimenti Diretti Barranin (IDB), u attwalment ma hemm l-ebda mekkaniżmu ta' skrinjar fil-livell tal-UE[193].

117 L-awtonomija strateġika akbar hija objettiv fl-Istrateġija Globali tal-UE u fil-Komunikazzjoni tal-2017 *Reżiljenza, Deterrenza u Difiża*[194]. L-indirizzar tal-għadd kbir ta' sfidi ppreżentati f'dan ir-rapport se jikkontribwixxi għat-tisħiħ ta' din l-awtonomija mixtieqa. L-ebda miżura unika mhi se tikseb dan waħidha.

Punti ta' riflessjoni – Rispons effettiv

- Id-Direttiva NIS kif tejbet in-notifika ta' inċidenti ċibernetiċi f'setturi kritiċi u lil hinn minnhom?
- L-istituzzjonijiet tal-UE kemm qed jinternalizzaw tajjeb il-koordinazzjoni tar-rispons għall-kriżijiet għal inċident ċibernetiku kbir?
- Iċ-ċiberdiplomazija kif jista' jkollha rwol prominenti fl-azzjonijiet esterni tal-UE?
- L-istrutturi u l-azzjonijiet attwali tal-UE jindirizzaw id-diżinformazzjoni proporzjonata għall-iskala u l-kumplessità tal-problema?

Kummenti finali

118 Fi snin reċenti, l-UE u l-Istati Membri tagħha mexxew iċ-ċibersigurtà 'l quddiem fl-aġenda sabiex itejbu r-reżiljenza ċibernetika kumplessiva. Madankollu, l-ilħuq ta' livell ogħla ta' ċibersigurtà fl-Unjoni jibqa' impenn monumentali. F'dan id-dokument informattiv u analitiku, aħna kellna l-għan li niġbdu l-attenzjoni għall-isfidi prinċipali għall-ambizzjoni tal-UE li ssir l-ambjent diġitali l-aktar sikur fid-dinja.

119 L-analiżi tagħna turi li tinħtieġ bidla lejn kultura tal-prestazzjoni li tinkorpora prattiki ta' evalwazzjoni għall-iżgurar ta' **obbligu ta' rendikont u ta' evalwazzjoni** siewja. **Għad baqa' xi lakuni fid-dritt, u l-leġiżlazzjoni eżistenti ma tiġix trasposta b'mod konsistenti mill-Istati Membri**. Dan jista' jagħmilha diffiċli għal-leġiżlazzjoni biex tilħaq il-potenzjal sħiħ tagħha. Sfida oħra li ġiet identifikata tirrigwarda l-**allinjament tal-livelli ta' investiment mal-għanijiet strateġiċi**, li jappella għaż-żieda fil-livelli ta' investiment u l-impatt tagħha. Dan huwa aktar diffiċli meta l-UE u l-Istati Membri tagħha ma jkollhomx **stampa ġenerali ċara tal-infiq tal-UE** fil-qasam taċ-ċibersigurtà. Hemm ukoll **limitazzjonijiet irrappurtati fil-forniment ta' riżorsi adegwati tal-aġenziji rilevanti għaċ-ċiberspazju tal-UE**, inklużi diffikultajiet fl-attrazzjoni u ż-żamma ta' talent.

120 Studji disponibbli jikkonkludu li l-**governanza taċ-ċibersigurtà tista' tissaħħaħ** biex tagħti spinta lill-abbiltà tal-komunità globali li tirreaġixxi għal ċiberattakki u inċidenti. Fl-istess waqt, il-prevenzjoni tal-attakki kollha hija impossibbli. Għalhekk, l-**identifikazzjoni u r-rispons rapidi** kif ukoll il-**protezzjoni tal-infrastruttura kritika u l-funzjonijiet tas-soċjetà**, flimkien ma' **skambju ta' informazzjoni u koordinazzjoni** aħjar bejn is-settur pubbliku u dak privat huma sfidi ewlenin li jridu jiġu indirizzati. Fl-aħħar nett, in-nuqqas globali dejjem akbar ta' ħiliet fil-qasam taċ-ċibersigurtà jfisser li **ż-żieda tal-ħiliet u s-sensibilizzazzjoni** fis-setturi u l-livelli kollha tas-soċjetà huma wkoll sfida importanti.

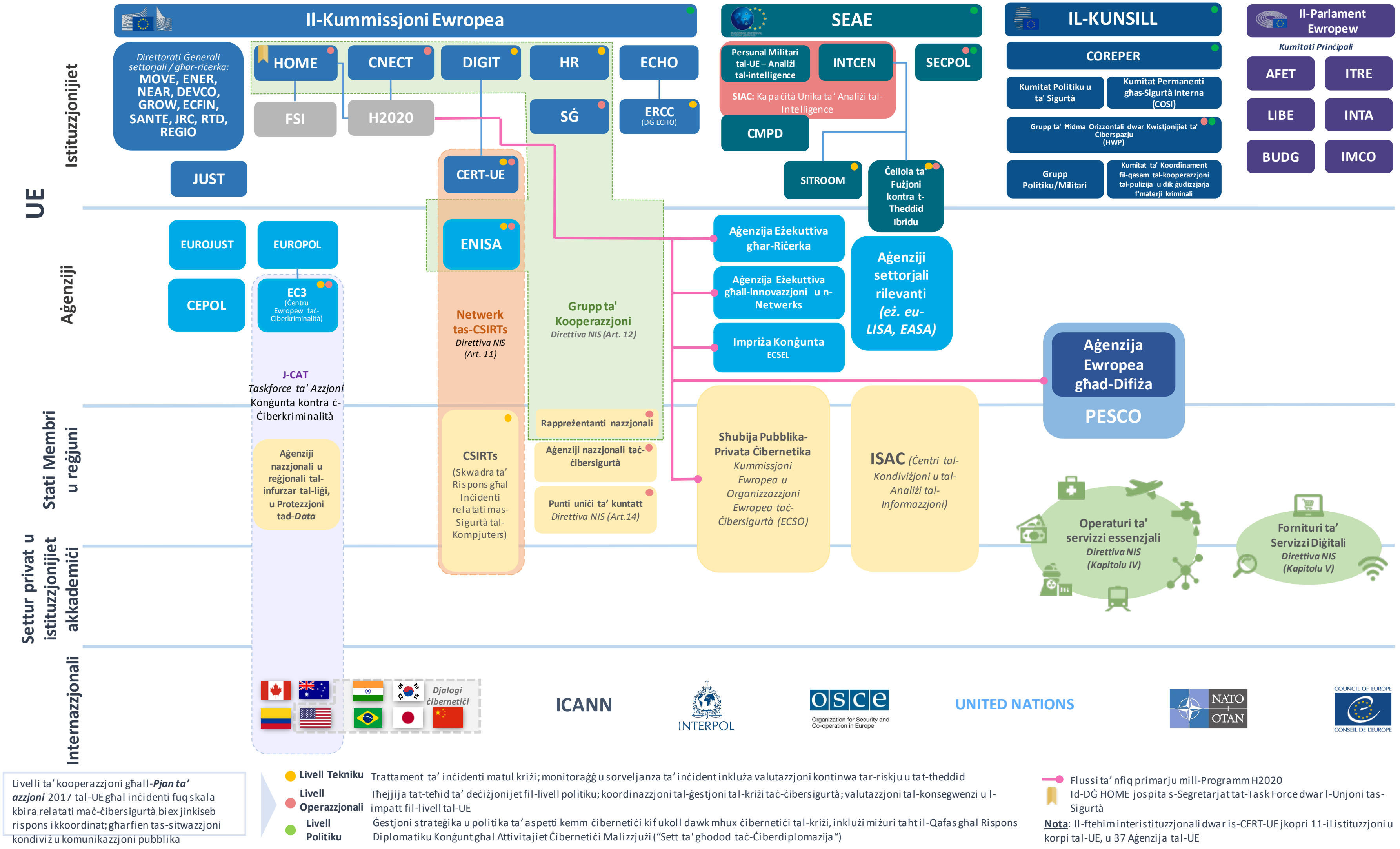
121 Dawn l-isfidi ppreżentati mit-theddid ċibernetiku li l-UE u l-ambjent globali ġenerali qed jiffaċċjaw, jirrikjedu impenn kontinwat u aderenza soda u kontinwa mal-valuri tal-UE.

Dan id-Dokument Informattiv u Analitiku ġie adottat mill-Awla III fil-laqgħa tagħha tal-14 ta' Frar 2019.

Għall-Qorti Ewropea tal-Awdituri

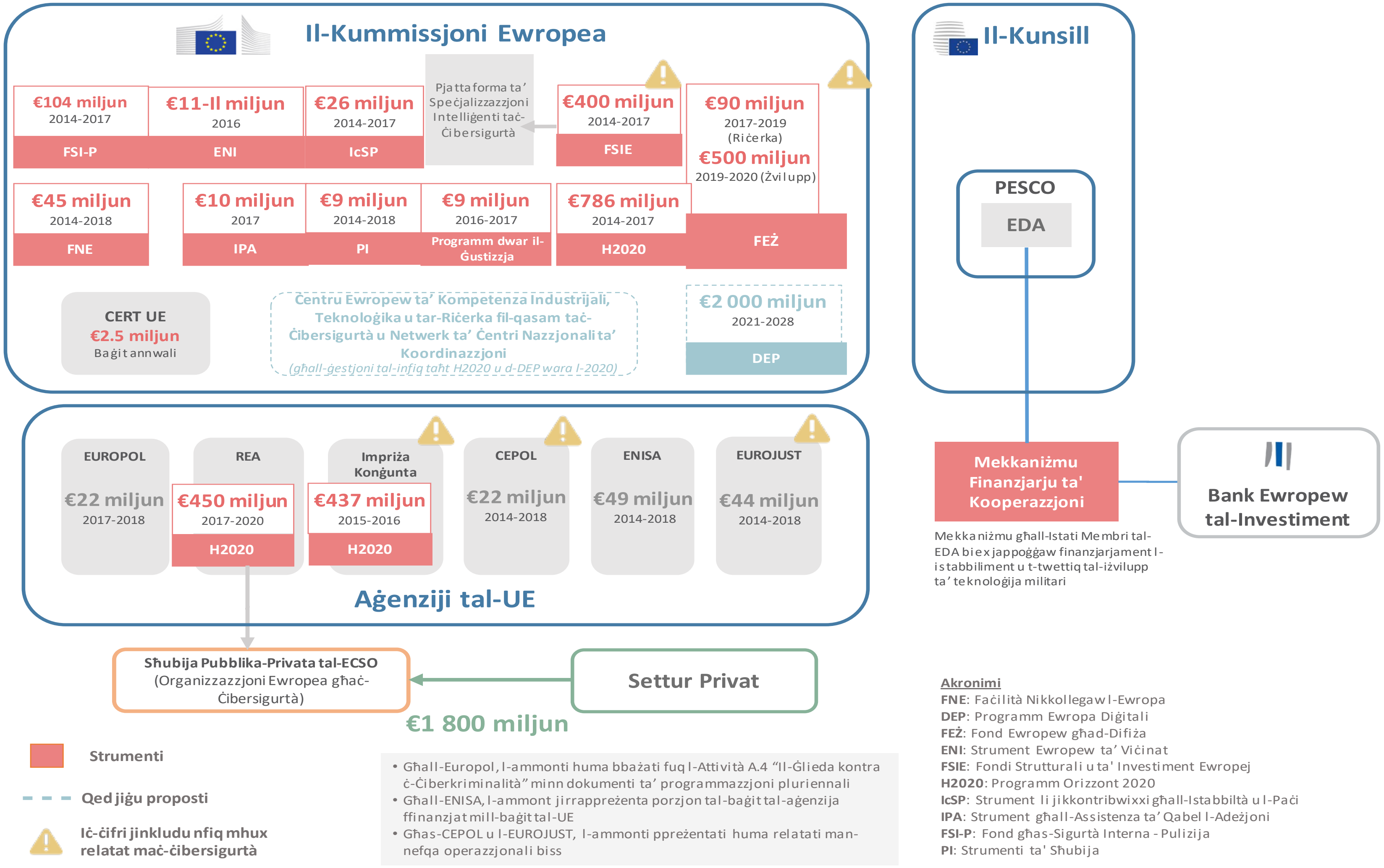
Klaus-Heiner Lehne
President

Anness I — Xenarju kumpless u b'diversi livelli li jinkludi ħafna atturi



Sors: Il-QEA.

Anness II — Infiq tal-UE fuq iċ-ċibersigurtà mill-2014 'il hawn



Sors: Il-QEA, ibbażat fuq dokumenti tal-Kummissjoni Ewropea u l-aġenziji tal-UE.

Anness III — Rapporti mill-uffiċċji tal-awditjar tal-Istati Membri tal-UE

Tip	Titlu (bl-iperlink)	Sena	SM
Awditi tal-konformità	Nota tal-valutazzjoni tal-Kontroll Intern	2014	FR
	Rapport ta' Ċertifikazzjoni għall-kontijiet tal-Iskema Ġenerali tas-Sigurtà Soċjali (difiża, affarijiet barranin)	2016	FR
	Ċertifikazzjoni tal-kontijiet tal-Istat	2016	FR
	Żgurar tas-sigurtà u l-preservazzjoni ta’ databases nazzjonali Estonjani ta’ importanza kritika	Intemm fl-2018 / għadu ma ġiex ippubblikat	EE
	Effettività ta’ kontrolli interni fil-protezzjoni ta’ *data* personali fid-databases nazzjonali	2008	EE
Awditi tal-prestazzjoni / li jivverifikaw il-valur għall-flus	Rapport dwar il-mitigazzjoni taċ-ċiberattakki	2013	DK
	RiR 2014:23 Sigurtà tal-Informazzjoni fl-amministrazzjoni pubblika ċivili	2014	SE
	Rapport dwar l-ipproċessar mill-gvern ta’ *data* kunfidenzjali dwar il-persuni u l-kumpaniji	2014	DK
	Il-Programm Nazzjonali taċ-Ċibersigurtà	2014	UK
	Rapport għall-Kumitat tal-Baġit tal-Parlament Federali Ġermaniż skont l-Artikolu 88, il-paragrafu 2, tal-Kodiċi tal-Baġit Federali (BHO) – konsolidazzjoni tal-IT, il-Gvern Federali	2015	DE
	Rapport dwar l-aċċess għas-sistemi tal-IT li jappoġġaw il-provvediment ta’ servizzi essenzjali lis-soċjetà Daniża	2015	DK
	Awtorità tal-Ippjanar Pubbliku ta’ Plaine de France	2015	FR
	“Ambjent taċ-Ċibersigurtà fil-Litwanja” Verżjoni Litwana sommarju tradott fl-Ingliż	2015	LT
	Prestazzjoni ta’ kompiti relatati maċ-ċibersigurtà minn korpi pubbliċi fil-Polonja (bil-PL)	2015	PL
	RiR 2015:21 Ċiberkriminalità – il-pulizija u l-prosekuturi jistgħu jkunu aktar effiċjenti.	2015	SE
	Diskrepanza fil-Ħiliet Diġitali fil-Gvern (Stħarriġ)	2015	UK
	Rapport għall-Parlament Federali: Finanzi Federali: ġbir tat-taxxa tas-suċċessjoni	2016	BE
	Rapport dwar il-ġestjoni tas-sigurtà tal-IT f’sistemi esternalizzati lil fornituri esterni	2016	DK
	Rapport tal-awditjar tal-attività ta’ self tal-Istitut tal-Kreditu Uffiċjali 2016	2016	ES
	Tmexxija tan-Netwerk tas-Sigurtà tal-Gvern	2016	FI
	Żgurar tas-sigurtà tas-sistemi tal-IT użati għall-kompiti pubbliċi	2016	PL
	Prevenzjoni u ġlieda kontra l-bullying ċibernetiku fost it-tfal u fost il-persuni	2016	PL
	Xogħol ta’ sigurtà tal-informazzjoni f’disa’ aġenziji - Awditu ieħor tas-sigurtà tal-informazzjoni fl-Istat. RiR 2016:8	2016	SE

Tip	Titlu (bl-iperlink)	Sena	SM
	Protezzjoni tal-informazzjoni fil-gvern kollu	2016	UK
	Rapport dwar il-protezzjoni tas-sistemi tal-IT u ta' *data* dwar is-saħħa fi tliet reġjuni Daniżi	2017	DK
	Nota dwar ir-riżultati tal-awditu parallel internazzjonali "Effettività ta' kontrolli interni fil-protezzjoni ta' *data* personali f'databases nazzjonali.	2017	EE
	Arranġamenti ta' protezzjoni ċibernetika	2017	FI
	Tmexxija tal-affidabbiltà ta' servizzi elettroniċi	2017	FI
	Netwerk tal-kmamar tal-Agrikoltura (sinteżi)	2017	FR
	Vaucluse Kamra tal-Kummerċ u l-Industrija (mill-Awla tal-Awditjar Reġjonali PACA)	2017	FR
	Żgurar tas-sigurtà u l-preservazzjoni ta' databases nazzjonali Estonjani ta' importanza kritika	Intemm fl-2018 / għadu ma ġiex ippubblikat	EE
	"Żvilupp tal-Infrastruttura ta' Komunikazzjoni Elettronika tal-Istat" Verżjoni Litwana sommarju tradott fl-Ingliż	2017	LT
	Awditu tat-Teknoloġija tal-Informazzjoni: Ċibersigurtà fl-Entitajiet tal-Gvern	2017	MT
	Is-sistema nazzjonali tar-reġistri: sigurtà, prestazzjoni u faċilità tal-użu	2017	PL
	L-inċident ta' *WannaCry*	2017	UK
	Frodi Online	2017	UK
	Rapport dwar il-protezzjoni kontra l-attakki minn software ta' riskatt	2018	DK
	Sptar ta' Arpajon (ħdejn il-Kamra Reġjonali ta' Île-de-France)	2018	FR
	"Ġestjoni ta' Riżorsi ta' Informazzjoni fi Stat Kritiku"	2018	LT
	"Kriminalità Elettronika"	2019	LT
	Sigurtà tal-Informazzjoni fil-Polonja	2019	PL
Oħrajn	Database tal-korpi pubbliċi	m/a	BE
	Kwestjonarju dwar il-politika ta' sigurtà u l-analiżi tar-riskju (għadu għaddej)	m/a	BE

Akronimi u abbrevjazzjonijiet

ASE: Awtorità Superviżorja Ewropea

CERT-UE: Skwadra ta' Rispons f'Emerġenza relatata mal-Kompjuters

cPPP: Sħubija Pubblika-Privata kuntrattwali

CSIRT: Skwadra ta’ Rispons għal Inċidenti relatati mas-Sigurtà tal-Kompjuters

DDoS: Attakk Distribwit li Jwaqqaf is-Servizz

DEP: Programm Ewropa Diġitali

DĠ CONNECT: Netwerks tal-Komunikazzjonijiet, Kontenut u Teknoloġija

DĠ HOME: Direttorat Ġenerali għall-Migrazzjoni u l-Affarijiet Interni

DĠ JUST: Direttorat Ġenerali għall-Ġustizzja u l-Konsumaturi

DIGIT: Direttorat Ġenerali għall-Informatika

Direttiva NIS: Direttiva dwar is-Sigurtà tan-Netwerks u tal-Informazzjoni

EC3: Ċentru Ewropew taċ-Ċiberkriminalità tal-Europol

ECSEL: Komponenti u Sistemi Elettroniċi għat-Tmexxija Ewropea

ECSM: Xahar iddedikat għaċ-Ċibersigurtà Ewropea

ECSO: Organizzazzjoni Ewropea taċ-Ċibersigurtà

EDA: Aġenzija Ewropea għad-Difiża

ENISA: Aġenzija Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni

FSI - P: Fond għas-Sigurtà Interna - Pulizija

FSIE: Fondi Strutturali u ta’ Investiment Ewropej

GDPR: Regolament Ġenerali dwar il-Protezzjoni tad-*Data*

HWPCI: Grupp ta' Ħidma Orizzontali dwar Kwistjonijiet ta' Ċiberspazju

ICS: Sistemi ta' Kontroll Industrijali

IDB: Investiment Dirett Barrani

ISSB: Bord ta' Tmexxija tas-Sigurtà tal-Informazzjoni

JRC: Ċentru Konġunt tar-Riċerka

LISO: Uffiċjal Lokali tas-Sigurtà tal-Informazzjoni

NAO: Uffiċċju Nazzjonali tal-Awditjar

NCIRC: Kapaċità ta' rispons tan-NATO għal inċidenti relatati mal-kompjuters

PESCO: Qafas ta' Kooperazzjoni Strutturata Permanenti

PSDK: Politika ta’ Sigurtà u ta’ Difiża Komuni

QEA: Il-Qorti Ewropea tal-Awdituri

SEAE: Servizz Ewropew għall-Azzjoni Esterna

SME: Intrapriża Żgħira u ta' Daqs Medju

UE: Unjoni Ewropea

Glossarju

Adware: Software malizzjuż li juri strixxuni ta’ reklamar jew pop-ups li jinkludu kodiċi għas-sorveljanza tal-imġiba online tal-vittmi.

Attakk Distribwit li Jwaqqaf is-Servizz (DDoS): Ċiberattakk li jipprevieni lill-utenti leġittimi milli jkollhom aċċess għal servizz jew riżors online billi jintbagħtulhom aktar talbiet milli jifilħu.

Botnet: Netwerk ta’ kompjuters infettati b’software malizzjuż u kkontrollati mill-bogħod, mingħajr ma jindunaw l-utenti, biex tintbagħat posta elettronika spam, tinsteraq informazzjoni jew jitniedu ċiberattakki kkoordinati.

Ċiberattakk: Tentattiv biex jiddgħajfu jew jinqerdu l-kunfidenzjalità, l-integrità u d-disponibbiltà tad-*data* jew ta’ sistema tal-kompjuter permezz taċ-ċiberspazju.

Ċiberdifiża: Subsett taċ-ċibersigurtà li għandu l-għan li jiddefendi ċ-ċiberspazju b’mezzi militari u b’mezzi xierqa oħra sabiex jintlaħqu l-għanijiet strateġiċi militari.

Ċiberkriminalità: Diversi attivitajiet kriminali li jinvolvu kompjuters u sistemi tal-IT, bħala għodda primarja jew inkella mira primarja. Dawn l-attivitajiet jinkludu: reati tradizzjonali (eż. frodi, falsifikazzjoni u serq tal-identità); reati relatati mal-kontenut (eż. distribuzzjoni online ta’ pornografija tat-tfal jew inċitament għal mibegħda razzjali); u reati uniċi għall-kompjuters u s-sistemi ta’ informazzjoni (eż. attakki kontra s-sistemi ta’ informazzjoni, attakki li jwaqqfu s-servizz u malware).

Ċibersigurtà: Is-salvagwardji u l-miżuri kollha adottati biex jiddefendu s-sistemi tal-IT u d-*data* tagħhom kontra aċċess mhux awtorizzat, attakk u ħsara biex jiġu żgurati d-disponibbiltà, il-kunfidenzjalità u l-integrità tagħhom.

Ċiberspazju: L-ambjent globali intanġibbli li fih komunikazzjoni online sseħħ bejn persuni, software u servizzi permezz ta’ netwerks tal-kompjuter u apparat teknoloġiku.

Cloud computing: Il-forniment ta’ riżorsi tal-IT fuq talba – bħall-ħżin, il-qawwa komputazzjonali jew il-kapaċità ta' kondiviżjoni tad-data - fuq l-internet, permezz tal-ospitalità fuq servers remoti.

***Data* dwar l-aċċess:** Informazzjoni dwar l-attività ta’ log-in u log-out min-naħa ta’ utent biex jaċċessa servizz, bħal ħin, data u indirizz IP.

***Data* personali:** Informazzjoni relatata ma’ individwu identifikabbli.

Disponibbiltà: L-iżgurar li l-informazzjoni tiġi aċċessata u użata b'mod f'waqtu u affidabbli.

Diżinformazzjoni: Informazzjoni li tista' tiġi kkonfermata bħala falza jew qarrieqa, li tinħoloq, tiġi ppreżentata u disseminata għall-benefiċċju ekonomiku jew biex tqarraq intenzjonalment bil-pubbliku, u li tista' tikkawża ħsara pubblika.

Ekosistema ċibernetika: Komunità kumplessa ta' apparat, *data*, netwerks, persuni, proċessi, u organizzazzjonijiet li jinteraġixxu bejniethom, kif ukoll l-ambjent ta' proċessi u teknoloġiji li jinfluwenzaw u jappoġġaw dawn l-interazzjonijiet.

Ġestjoni tal-vulnerabbiltajiet: Parti integrali tas-sigurtà tal-kompjuters u n-netwerks biex jiġi mmitigat jew ipprevenut b'mod proattiv l-isfruttament tal-vulnerabbiltajiet tas-sistema u tas-software permezz tal-identifikazzjoni, il-klassifikazzjoni, u r-rimedju għalihom.

Hacker: Individwi jew gruppi li jiksbu aċċess mhux awtorizzat għal sistemi ta' informazzjoni jew netwerks bil-ħsieb li jsegwu għanijiet soċjali u politiċi.

Inċident ċibernetiku: Avveniment li jagħmel ħsara jew li jhedded b'mod dirett jew indirett ir-reżiljenza u s-sigurtà ta' sistema tal-IT u d-*data* li hija tipproċessa, taħżen jew tittrażmetti.

Infrastruttura elettorali: Tinkludi sistemi tal-IT u databases għall-kampanji, informazzjoni sensittiva dwar il-kandidati, sistemi ta' reġistrazzjoni u ta' ġestjoni tal-votanti.

Infrastruttura kritika: Riżorsi fiżiċi, servizzi, u faċilitajiet li t-tfixkil jew il-qerda tagħhom ikollhom impatt serju fuq il-funzjonament tal-ekonomija u s-soċjetà.

Integrità: Il-ħarsien kontra l-modifiki mhux xierqa jew il-qerda tal-informazzjoni, u l-garanzija tal-awtentiċità tagħha.

Internet tal-Oġġetti: In-netwerk tal-oġġetti ta' kuljum mgħammra b'elettronika, software u sensuri, biex b'hekk ikun hemm komunikazzjoni u skambju ta' *data* fuq l-internet.

Kitt ta' sfruttament: Tip ta' sett ta' għodod li ċ-ċiberkriminali jużaw biex jattakkaw il-vulnerabbiltajiet fis-sistemi ta' informazzjoni, biex b'hekk ikunu jistgħu jiddistribwixxu malware jew iwettqu attivitajiet malizzjużi oħra.

Kontenut diġitali: Kwalunkwe *data* – bħal test, ħoss, stampi jew vidjo – maħżuna f'format diġitali.

Kriminalità bl-użu tal-internet: Kriminalità tradizzjonali mwettqa fuq skala akbar bl-użu ta' sistemi tal-IT.

Kriminalità ċiberdipendenti: Kriminalità li tista' titwettaq biss bl-użu ta' apparat tal-IT.

Kriptaġġ: It-trasformazzjoni ta' informazzjoni li tinqara f'kodiċi li ma jinqarax biex din tiġi protetta. Biex jaqra l-informazzjoni, l-utent irid ikollu aċċess għal kjavi sigrieta jew password.

Kriptovaluta: Assi diġitali li jinħareġ u jiġi skambjat bl-użu ta' tekniki ta' kriptaġġ, indipendentement minn bank ċentrali. Huwa aċċettat bħala mezz ta' pagament fost il-membri ta' komunità virtwali.

Kunfidenzjalità: Il-protezzjoni ta' informazzjoni, *data* jew assi kontra aċċess jew divulgazzjoni mhux awtorizzati.

Malware li jħassar id-*data* (Wiper malware): Klassi ta' malware li l-intenzjoni tiegħu hija li jħassar id-*data* minn fuq il-hard drive tal-kompjuter li jinfetta.

Malware: Software malizzjuż. Programm tal-kompjuter imfassal biex jagħmel ħsara lil kompjuter, server jew netwerk.

Mudell ta' reat kriminali bħala servizz (CaaS): Mudell ta' kummerċ kriminali li jixpruna l-ekonomija sotterranja diġitali, billi jipprovdi firxa wiesgħa ta' servizzi u għodod kummerċjali li jippermettu liċ-ċiberkriminali bla sengħa u li jinsabu fil-livell tad-dħul iwettqu ċiberkriminalità.

Phishing: Il-prattika li tintbagħat posta elettronika li tkunu tidher li toriġina minn sors fdat sabiex tqarraq bir-riċevituri biex jikklikkjaw fuq links malizzjużi jew jikkondividu informazzjoni personali.

Reżiljenza ċibernetika: L-abbiltà ta' prevenzjoni, tħejjija u reżistenza għal inċidenti u ċiberattakki, kif ukoll l-irkupru minnhom.

Servizzi fiduċjarji: Servizzi li jtejbu l-validità legali ta' tranżazzjoni elettronika, bħal firem elettroniċi, siġilli, kronogrammi, awtentikazzjoni ta' konsenja rreġistrata u ta' siti web.

Sigurtà tal-informazzjoni: Is-sett ta' proċessi u għodod li jipproteġu d-*data* fiżika u diġitali minn aċċess mhux awtorizzat, użu, divulgazzjoni, tfixkil, modifiki, reġistrazzjoni jew qerda.

Sigurtà tan-netwerks: Subsett taċ-ċibersigurtà li jipproteġi d-*data* li tintbagħat permezz ta’ apparat fuq l-istess netwerk, biex jiġi żgurat li l-informazzjoni ma tiġix interċettata jew mibdula.

Sistema ta' legat: Sistema tal-kompjuter, applikazzjoni jew lingwa ta' programmar obsoleti jew antikwati li għadhom jintużaw, iżda li għalhom l-aġġornamenti u l-appoġġ tal-bejjiegħa jistgħu ma jkunux disponibbli, inkluż l-appoġġ għas-sigurtà.

Skimming: Is-serq ta’ *data* dwar il-karti ta' kreditu jew ta' debitu meta din tiddaħħal online.

Social engineering: Fil-qasam tas-sigurtà tal-informazzjoni, il-manipulazzjoni psikoloġika sabiex persuni jiġu mqarrqa biex iwettqu azzjoni jew jiddivulgaw informazzjoni kunfidenzjali.

Software ta' riskatt : Software malizzjuż li ma jħallix lill-vittmi jkollhom aċċess għal sistema tal-kompjuter jew li permezz tiegħu l-fajls ma jkunux jistgħu jinqraw, normalment permezz ta’ kriptaġġ. L-aggressur imbagħad normalment jirrikatta lill-vittma billi jirrifjuta li jerġa’ jtih aċċess sakemm jitħallas riskatt.

Theddid ibridu: Espressjoni ta’ intenzjoni ostili li l-avversarji jagħmlu bl-użu ta’ taħlita ta' tekniki ta’ gwerra konvenzjonali u mhux konvenzjonali (jiġifieri metodi militari, politiċi, ekonomiċi u teknoloġiċi) fl-insegwiment qawwi tal-objettivi tagħhom.

Użu ta’ software korrettiv: L-introduzzjoni ta’ sett ta’ bidliet għas-software jew biex dan jiġi aġġornat, jissewwa, jew jittejjeb, inkluża t-tiswija ta’ vulnerabbiltajiet tas-sigurtà.

Vektorizzazzjoni tat-testi: Il-proċess ta’ konverżjoni ta’ kliem, sentenzi jew dokumenti sħaħ f’vetturi numeriċi biex b’hekk algoritmi tat-tagħlim awtomatiku jkunu jistgħu jużawhom.

[1] Fl-abbozz tal-Att dwar iċ-Ċibersigurtà tal-UE, din ġiet iddefinita bħala l-attivitajiet kollha meħtieġa biex jiġu protetti n-netwerks u s-sistemi ta' informazzjoni, l-utenti tagħhom, u persuni affettwati minn theddid ċibernetiku. L-Att huwa mistenni li jiġi adottat mill-Parlament Ewropew u mill-Kunsill fil-bidu tal-2019.

[2] L-Europol, *Internet Organised Crime Threat Assessment 2017* (Valutazzjoni tal-2017 dwar it-Theddida mill-Kriminalità Organizzata ffaċilitata mill-Internet).

[3] L-Organizzazzjoni Ewropea taċ-Ċibersigurtà (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership* (Proposta mill-Industrija Ewropea taċ-Ċibersigurtà għal Sħubija Pubblika-Privata kuntrattwali), Ġunju 2016.

[4] Il-Parlament Ewropew, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (Ċibersigurtà fl-Unjoni Ewropea u Lil hinn Minnha: Esplorazzjoni tat-Theddid u r-Rispons ta' Politika), Studju għall-Kumitat LIBE, Settembru 2015.

[5] L-ENISA, *ENISA Threat Landscape Report 2017* (Rapport dwar ix-Xenarju tat-Theddid tal-ENISA 2017), it-18 ta' Jannar 2018.

[6] L-Europol, *Internet Organised Crime Threat Assessment 2018* (Valutazzjoni tal-2018 dwar it-Theddida mill-Kriminalità Organizzata ffaċilitata mill-Internet).

[7] L-Europol, *Ibid.*, 2018.

[8] Iċ-Ċentru Ewropew għall-Ekonomija Politika, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (Serq tal-Ideat: Iċ-ċiberspjunaġġ se jkun jista' jżomm lura lill-Ewropa mit-tellieqa globali għall-kompetittività industrijali?), id-Dokument Okkażjonali Nru 2/18, Frar 2018.

[9] Il-Kummissjoni Ewropea, L-Istat tal-Unjoni 2017 tal-President.

[10] L-Europol, *World's Biggest Marketplace selling internet paralysing DDoS attacks taken down* (Ingħalaq l-Akbar Suq fid-Dinja li jbigħ attakki DDoS paralizzanti fuq l-internet), stqarrija għall-istampa, il-25 ta' April 2018.

[11] L-Europol, *Internet Organised Crime Threat Assessment 2017* (Valutazzjoni tal-2017 dwar it-Theddida mill-Kriminalità Organizzata ffaċilitata mill-Internet).

[12] L-iskeda informattiva tal-Kummissjoni Ewropea dwar iċ-ċibersigurtà, Settembru 2017.

[13] L-ispejjeż jistgħu jinkludu: telf fid-dħul, spejjeż għat-tiswija ta' sistemi bil-ħsara; obbligazzjonijiet potenzjali għal assi jew informazzjoni misruqa; inċentivi għaż-żamma tal-klijenti; primjums tal-assigurazzjoni ogħla; żieda fl-ispejjeż relatati mal-protezzjoni (sistemi ġodda, impjegati, taħriġ); riżoluzzjoni potenzjali tal-ispejjeż ta' konformità jew tal-litigazzjoni.

[14] NTT Security, *Risk:Value 2018 Report* (Riskju: Rapport dwar il-Valuri 2018).

[15] Is-software ta' riskatt *Wannacry* sfrutta l-vulnerabbiltajiet fi protokoll ta' Microsoft Windows, u dan ippermetta l-akkwiżizzjoni mill-bogħod ta' kull kompjuter. Il-kumpanija Microsoft ħarġet software korrettiv wara li kienet skopriet il-vulnerabbiltà. Madankollu, mijiet ta' eluf ta' kompjuters kienu għadhom ma ġewx aġġornati, u ħafna minn dawn ġew sussegwentement infettati. Sors: A. Greenberg, *Hold North Korea Accountable For*

Wannacry—and the NSA, too (Inżommu lill-Korea ta' Fuq Responsabbli għal *Wannacry* — u l-NSA wkoll), WIRED, id-19 ta' Diċembru 2017.

[16] Il-Kumissjoni Ewropea, *Europeans' attitudes towards cybersecurity* (L-attitudni tal-Ewropej lejn iċ-ċibersigurtà), l-Ewrobarometru Speċjali 464a, Settembru 2017. Stħarriġ ta' segwitu huwa mistenni li jiġi ppubblikat fil-bidu tal-2019.

[17] Il-Konvenzjoni ta' Budapest hija linja gwida internazzjonali vinkolanti għal pajjiżi li qed jiżviluppaw leġiżlazzjoni kontra ċ-ċiberkriminalità. Hija tipprovdi qafas għall-kooperazzjoni internazzjonali bejn l-Istati partijiet. Il-Kummissjoni, il-Kunsill tal-Unjoni Ewropea, l-Europol, l-ENISA u l-Eurojust attwalment jirrappreżentaw l-UE.

[18] Il-Kummissjoni Ewropea, *L-Istrateġija ta' Ċibersigurtà tal-Unjoni Ewropea: Ċiberspazju Miftuħ, Sikur u Sigur*, JOIN (2013) 1 final, is-7 ta' Frar 2013.

[19] Il-Kummissjoni Ewropea, *L-Aġenda Ewropea dwar is-Sigurtà*, COM(2015) 185 final, it-28 ta' April 2015.

[20] Il-Kummissjoni Ewropea, *Strateġija għal Suq Uniku Diġitali għall-Ewropa*, COM(2015) 192 final, is-6 ta' Mejju 2015.

[21] Is-SEAE, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy* (Viżjoni Kondiviża, Azzjoni Komuni: Ewropa Aktar b'Saħħitha. Strateġija Globali għall-Politika Estera u ta' Sigurtà tal-Unjoni Ewropea), Ġunju 2016.

[22] Iċ-Ċentru għall-Istudji Politiċi Ewropej, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Tisħiħ tal-Kapaċitajiet tal-UE għaċ-Ċiberdifiża – Rapport ta' Task Force tas-CEPS), Novembru 2018.

[23] Il-malware użat għall-attakk mis-software ta' riskatt *Wannacry* li ġie attribwit lill-Korea ta' Fuq mill-Istati Uniti, mir-Renju Unit u mill-Awstralja, oriġinarjament ġie żviluppat u akkumulat mill-Aġenzija tas-Sigurtà Nazzjonali tal-Istati Uniti biex jisfrutta l-vulnerabbiltajiet tal-Windows. Sors: A. Greenberg, *ibid.*, WIRED, id-19 ta' Diċembru 2017. Wara l-attakki, il-kumpanija Microsoft ikkundannat l-akkumulazzjoni ta' vulnerabbiltajiet tas-software mill-gvernijiet u tenniet it-talba tagħha għall-ħtieġa għal Konvenzjoni Diġitali ta' Ġinevra.

[24] Minbarra l-art, il-baħar, l-arja u l-ispazju.

[25] Il-Qafas ta' Politika tal-UE dwar iċ-Ċiberdifiża (aġġornament tal-2018), 14413/18, id-19 ta' Novembru 2018.

[26] Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *Qafas Konġunt biex jiġi miġġieled it-theddid ibridu: reazzjoni tal-Unjoni Ewropea*, JOIN(2016) 18 final, is-6 ta' April 2016.

[27] Dikjarazzjoni konġunta mill-Presidenti tal-Kunsill Ewropew u tal-Kummissjoni Ewropea, u mis-Segretarju Ġenerali tal-Organizzazzjoni tat-Trattat tal-Atlantiku tat-Tramuntana, it-8 ta' Lulju 2016 u l-10 ta' Lulju 2018.

[28] Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *Reżiljenza, Deterrenza u Difiża: Il-bini ta' ċibersigurtà b'saħħitha għall-UE*, JOIN(2017) 450 final, it-13 ta' Settembru 2017.

[29] Id-Direttiva (UE) 2016/1148 tal-Parlament Ewropew u tal-Kunsill tas-6 ta' Lulju 2016 dwar miżuri għal livell għoli komuni ta' sigurtà tan-netwerks u tas-sistemi tal-informazzjoni madwar l-Unjoni (ĠU L 194, 19.7.2016, p. 1).

[30] Id-Direttiva (UE) 2016/1148 tal-Parlament Ewropew u tal-Kunsill tas-6 ta' Lulju 2016 dwar miżuri għal livell għoli komuni ta' sigurtà tan-netwerks u tas-sistemi tal-informazzjoni madwar l-Unjoni.

[31] Dawn jiġu integrati fi strutturi kooperattivi stabbiliti mid-direttiva, fin-Netwerk tas-CSIRTs (netwerk magħmul minn CSIRTs maħtura mill-Istati Membri tal-UE u minn CERT-UE; l-ENISA tospita s-segretarjat) u fil-Grupp ta' Kooperazzjoni (jappoġġa u jiffaċilita l-kooperazzjoni strateġika u l-iskambju ta' informazzjoni fost l-Istati Membri li għalihom il-Kummissjoni tospita s-segretarjat).

[32] Ir-Regolament (UE) 2016/679 tal-Parlament Ewropew u tal-Kunsill tas-27 ta' April 2016 dwar il-protezzjoni tal-persuni fiżiċi fir-rigward tal-ipproċessar ta' *data* personali u dwar il-moviment liberu ta' tali *data*, u li jħassar id-Direttiva 95/46/KE (Regolament Ġenerali dwar il- Protezzjoni tad-*Data*) (ĠU L 119, 4.5.2016, p. 1).

[33] Il-Kummissjoni Ewropea, *Proposta għal regolament tal-Parlament Ewropew u tal-Kunsill dwar l-ENISA, l-"Aġenzija tal-UE għaċ-Ċibersigurtà" li jħassar ir-Regolament (UE) 526/2013, u li jikkonċerna ċ-Ċertifikazzjoni taċ-Ċibersigurtà tat-Teknoloġija tal-Informazzjoni u tal-Komunikazzjoni ("l-Att dwar iċ-Ċibersigurtà")*, COM(2017) 477 final, it-13 ta' Settembru 2017.

[34] Il-Kummissjoni Ewropea, *Proposta għal regolament tal-Parlament Ewropew u tal-Kunsill dwar l-Ordnijiet ta' Produzzjoni u ta' Preservazzjoni Ewropej għall-evidenza elettronika f'materji kriminali*, COM(2018) 225 final, is-17 ta' April 2018.

[35] Il-Kummissjoni Ewropea, *Proposta għal direttiva tal-Parlament Ewropew u tal-Kunsill li tistabbilixxi regoli armonizzati dwar il-ħatra ta' rappreżentanti legali għall-finijiet tal-ġbir tal-evidenza fi proċeduri kriminali*. COM(2018) 226 final, is-17 ta' April 2018.

[36] Il-Kummissjoni Ewropea, *Proposta għal regolament tal-Parlament Ewropew u tal-Kunsill li jistabbilixxi ċ-Ċentru Ewropew ta' Kompetenza Industrijali, Teknoloġika u tar-Riċerka fil-qasam taċ-Ċibersigurtà u n-Netwerk ta' Ċentri Nazzjonali ta' Koordinazzjoni*, COM(2018) 630 final, it-12 Settembru 2018.

[37] H. Carrapico u A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?* (L-UE bħala Attur Koerenti tas-Sigurtà/taċ-Ċibersigurtà), il-Ġurnal tal-Istudji tas-Suq Komuni, Vol. 55, Nru 6, 2017.

[38] Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta' Settembru 2017.

[39] Is-Servizz ta' Riċerka tal-Parlament Ewropew, *Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects* (Ċiberinsigurtà u ċiberkriminalità transatlantiċi. Impatt eknomiku u prospetti futuri), PE 603.948, Diċembru 2017.

[40] L-ENISA, *An evaluation framework for Cyber Security Strategies* (Qafas ta' evalwazzjoni għall-Istrateġiji ta' Ċibersigurtà), is-27 ta' Novembru 2014.

[41] Eċċezzjoni hija l-Artikolu 14 ("Monitoraġġ u statistika") tad-Direttiva 2013/40/UE tal-Parlament Ewropew u tal-Kunsill tat-12 ta' Awwissu 2013 dwar attakki kontra s-sistemi tal-informazzjoni u li tissostitwixxi d-Deċiżjoni Qafas tal-Kunsill 2005/222/ĠAI.

[42] Il-Kumitat Ekonomiku u Soċjali Ewropew, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks* (Ċibersigurtà: żgurar tas-sensibilizzazzjoni u r-reżiljenza tas-settur privat fl-Ewropa kollha fid-dawl tar-riskji ċibernetiċi li qed jiżdiedu), Marzu 2018. It-Task Force tas-CEPS-ECRI, Cybersecurity in Finance: Getting the policy mix right! (Ċibersigurtà fil-Finanzi: Kisba ta' riżultati tajbin fit-taħlita ta' politiki), Ġunju 2018.

[43] Minn 28 uffiċċju nazzjonali tal-awditjar, 24 irrispondew għall-istħarriġ tagħna.

[44] Dan ifisser li jkun ibbażat fuq il-prinċipji u kemm jista' jkun teknoloġikament newtrali.

[45] Il-Mekkaniżmu għall-Pariri Xjentifiċi tal-Kummissjoni Ewropea Scientific Opinion 2/2017 (Opinjoni Xjentifika Nru 2/2017), l-24 ta' Marzu 2017.

[46] L. Rebuffi, *EU Digital Autonomy: A possible approach* (Awtonomija Diġitali tal-UE: Approċċ possibbli), Digma Zeitschrift für Datenrecht und Informationssicherheit, Settembru 2018. Iċ-Ċentru Ewropew għall-Ekonomija Politika, *ibid.*, id-Dokument Okkażjonali Nru 2/18, Frar 2018.

[47] Il-Kummissjoni Ewropea, *Proposta għal Direttiva tal-Parlament Ewropew u tal-Kunsill dwar ċerti aspetti li jikkonċernaw il-kuntratti għall-provvista ta' kontenut diġitali*, COM(2015) 634 final, id-9 ta' Diċembru 2015.

[48] Il-Kummissjoni Ewropea, *Proposta għal Direttiva tal-Parlament Ewropew u tal-Kunsill dwar ċerti aspetti li jirrigwardaw il-kuntratti għall-bejgħ onlajn u bejgħ mill-bogħod ieħor ta' oġġetti*, COM(2015) 635 final, id-9 ta' Diċembru 2015.

[49] Il-Kunsill tas-Sigurtà Ċibernetika tan-Netherlands, *Laqgħa dwar il-Prospettiva Ewropea għaċ-Ċibersigurtà tal-2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care* (Rakkomandazzjonijiet akkademiċi mis-settur pubbliku u dak privat lill-Kummissjoni Ewropea dwar l-Internet tal-Oġġetti u l-Armonizzazzjoni ta' dmirijiet ta' diliġenza), 2016.

[50] Iċ-Ċentru għall-Istudji Politiċi Ewropej, *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges – Report of a CEPS Task Force* Divulgazzjoni tal-Vulnerabbiltajiet tas-Software fl-Ewropa: Tekonoloġija, Politiki u Sfidi Legali – Rapport ta' Task Force tas-CEPS), Ġunju 2018.

[51] Il-Kummissjoni Ewropea, *Nagħmlu l-aħjar użu min-NIS – lejn l-implimentazzjoni effettiva tad-Direttiva (UE) 2016/1148 dwar miżuri għal livell għoli komuni ta' sigurtà tan-netwerks u tas-sistemi tal-informazzjoni madwar l-Unjoni*, COM(2017) 476 final/2, l-4 ta' Ottubru 2017.

[52] L-Europol, *ibid.*, 2017.

[53] Il-Kunsill tal-Unjoni Ewropea, *Rapport finali dwar is-seba' ċiklu ta' evalwazzjonijiet reċiproċi dwar "L-implimentazzjoni u l-operazzjoni prattika tal-politiki Ewropej dwar il-prevenzjoni taċ-ċiberkriminalità u l-ġlieda kontriha"*, 12711/1/17 REV 1, id-9 ta' Ottubru 2017.

[54] Il-Kummissjoni Ewropea, "Impact assessment accompanying the document Proposal for a Directive on combating fraud and counterfeiting of non-cash means of payment" (Valutazzjoni tal-Impatt li takkumpanja l-Proposta għal Direttiva dwar il-ġlieda kontra l-frodi u l-falsifikazzjoni ta' mezzi ta' pagament mhux bi flus kontanti), SWD/2017/0298 final, it-13 ta' Settembru 2017. F'Diċembru 2018, intlaħaq ftehim politiku dwar il-leġiżlazzjoni l-ġdida, u huwa mistenni li jiġi adottat fil-bidu tal-2019.

[55] L-Europol, *ibid.*, 2017.

[56] C-362/14: Maximillian Schrems vs Data Protection Commissioner (l-Irlanda), is-6 ta' Ottubru 2015.

[57] L-Europol/l-Eurojust, *Common challenges in combatting cybercrime* (Sfidi komuni fil-ġlieda kontra ċ-ċiberkriminalità), 7021/17, it-13 ta' Marzu 2017.

[58] Il-Kummissjoni Ewropea, *Assessment of the EU 2013 Cybersecurity Strategy* (Valutazzjoni tal-Istrateġija tal-UE għaċ-Ċibersigurtà tal-2013), SWD (2017) 295 final, it-13 ta' Settembru 2017.

[59] Is-Servizz ta' Riċerka tal-Parlament Ewropew, *Briefing: EU Legislation in Progress – Review of dual-use export controls PE589.832* (Tgħarrif: Leġiżlazzjoni tal-UE li għadha qed titfassal – Analiżi tal-kontrolli tal-esportazzjoni ta' oġġetti b'użu doppju, PE589.832).

[60] Ir-Riżoluzzjoni tal-Parlament Ewropew, *Drittijiet tal-bniedem u teknoloġija: l-impatt ta' sistemi ta' intrużjoni u sorveljanza fuq id-drittijiet tal-bniedem f'pajjiżi terzi*, (2014/2232(INI)), it-8 ta' Settembru 2015. Prodotti u servizzi b'użu doppju, li jinkludu software u teknoloġija, jista' jkollhom applikazzjonijiet ċivili u militari.

[61] L-informazzjoni disponibbli għall-pubbliku tinħażen fid-database WHOIS, li hija mmaniġġjata mill-ICANN (Korporazzjoni tal-Internet dwar l-Ismijiet u n-Numri Assenjati). L-ICANN tieħu ħsieb is-Sistema tal-Ismijiet tad-Dominji. L-użu ħażin tal-ismijiet tad-dominji jiffaċilita ċ-ċiberkriminalità.

[62] L-Artikolu 3, id-Direttiva NIS, *ibid.*

[63] Il-Kunsill tal-Atlantiku, *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures* (Rabta bejn ir-Riskji: Ġejt mgħobbi b'riskji ċibernetiċi? Benefiċċji u spejjeż ekonomiċi ta' futuri ċibernetiċi alternanti), l-10 ta' Settembru 2015.

[64] Il-White House, *Cybersecurity spending fiscal year 2019* (Infiq fuq iċ-ċibersigurtà, is-sena fiskali 2019).

[65] Il-Kummissjoni Ewropea, *Commission Staff Working Document: 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'* (Dokument ta' Ħidma tal-Persunal tal-Kummissjoni: Valutazzjoni tal-Impatt li Takkumpanja d-dokument "Proposta għal Regolament tal-Parlament Ewropew u tal-Kunsill li jistabbilixxi

l-programm Ewropa Diġitali għall-perjodu 2021-2027), SWD(2018) 305 final, is-6 ta' Ġunju 2018.

66 Iċ-Ċentru tal-Aja għall-Istudji Strateġiċi, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Investimenti tan-Netherlands fl-ICT u fiċ-ċibersigurtà: inpoġġu dan f'perspettiva), Diċembru 2016.

67 Il-Kummissjoni Ewropea, *ibid.*, COM(2018) 630 final, it-12 ta' Settembru 2018.

68 L-Unità tal-Prospettiva Xjentifika tas-Servizz ta' Riċerka tal-Parlament Ewropew, *Achieving a sovereign and trustworthy ICT industry in the EU* (Ksib ta' industrija sovrana u affidabbli tal-ICT fl-UE), Diċembru 2017.

69 L-Alleanza Ewropea tal-SMEs Diġitali, *Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem* (Dokument ta' Pożizzjoni dwar l-Istrateġija Ewropea ta' Ċibersigurtà: Trawwim tal-ekosistema tal-SMEs), il-31 ta' Lulju 2017.

70 L-Unità tal-Prospettiva Xjentifika tas-Servizz ta' Riċerka tal-Parlament Ewropew, *ibid.*, Diċembru 2017.

71 *Ibid*.

72 Il-Kummissjoni Ewropea, *Valutazzjoni tal-impatt dwar il-proposta għal ċentru ta' kompetenza tar-riċerka u n-netwerk ta' ċentri nazzjonali ta' koordinazzjoni*, SWD(2018) 403 final (il-Parti 1/4), it-12 ta' Settembru 2018.

73 Il-Kummissjoni Ewropea, *ibid.*, COM(2018) 630 final, it-12 ta' Settembru 2018.

74 Ir-Rapport Speċjali Nru 13/2018 tal-QEA: "Il-ġlieda kontra r-radikalizzazzjoni li twassal għat-terroriżmu".

75 Iċ-ċifri kkwotati f'din it-taqsima jiġu minn dokumenti tal-Kummissjoni li huma disponibbli għall-pubbliku, ħlief għall-ammont ta' EUR 42 miljun li jissemma fil-paragrafu ***51***, li l-Kummissjoni pprovditilna b'mod dirett.

76 Orizzont 2020 huwa l-programm tal-UE għar-riċerka u l-innovazzjoni b'ammont ta' EUR 80 biljun, li jappoġġa l-Innovazzjoni tal-Unjoni u li huwa mmirat lejn l-iżgurar tal-kompetittività globali tal-UE.

77 L-Isfida Soċjetali 7 ta' Orizzont 2020 "Soċjetajiet Siguri u Innovattivi: protezzjoni tal-libertà u s-sigurtà tal-Ewropa u ċ-ċittadini tagħha".

78 Aħna analizzajna proġetti ta' H2020 mis-sett tad-*data* CORDIS. Aħna wettaqna vektorizzazzjoni tat-test fuq id-deskrizzjoni ta' kull proġett, bl-użu ta' tassonomija taċ-ċibersigurtà tal-JRC (ara l-***Kaxxa 5*** fil-kapitolu li jmiss), biex nidentifikaw proġetti li x'aktarx kienu relatati maċ-ċibersigurtà. Aħna mbagħad iċċekkjajna u analizzajna r-riżultati manwalment.

79 L-Organizzazzjoni Ewropea taċ-Ċibersigurtà, *ECS cPPP Progress Monitoring Report 2016-2017* (Rapport ta' Monitoraġġ tal-Progress tal-ECS cPPPs għall-perjodu 2016-2017), id-29 ta' Ottubru 2018.

80 L-Artikolu 9(2), id-Direttiva NIS, *ibid.*

[81] GLACY+ (l-Azzjoni Globali dwar iċ-Ċiberkriminalità+) hija proġett konġunt mal-Kunsill tal-Ewropa. Hija tappoġġa 12-il pajjiż fl-Afrika, fl-Asja-Paċifiku, kif ukoll fl-Amerka Latina u fir-reġjun tal-Karibew, li min-naħa tagħhom jistgħu jservu bħala hubs biex jikkondividu l-esperjenzi tagħhom fi ħdan ir-reġjuni rispettivi tagħhom.

[82] Iċ-Ċentru Ewropew ta' Strateġija Politika (ĊESP), il-grupp ta' riflessjoni tal-Kummissjoni, ikkummenta dwar ir-riskju li jirriżulta "punt moħbi diġitali" jekk id-diskrepanza bejn l-UE u l-viċinat tal-Balkani tal-Punent tagħha tkompli tikber. Pajjiżi bħaċ-Ċina u r-Russja qed jinvestu ammonti sinifikanti fir-reġjun, li għandu r-riskju li jimmarġinalizza l-UE bħala attur ċibernetiku fir-reġjun. Sors: Iċ-ĊESP, *Engaging with the Western Balkans: an investment in Europe's security* (Involviment mal-Balkani tal-Punent: investiment fis-sigurtà tal-Ewropa), is-17 ta' Mejju 2018.

[83] Il-Bank Ewropew tal-Investiment, *The EIB Group Operating Framework and Operational Plan 2018* (Il-Qafas Operattiv u l-Pjan Operazzjonali 2018 tal-Grupp tal-BEI), it-12 ta' Diċembru 2017. Ma kienx hemm aktar informazzjoni disponibbli fiż-żmien tal-abbozzar.

[84] Il-Kummissjoni Ewropea, *Proposta għal Regolament tal-Parlament Ewropew u tal-Kunsill li jistabbilixxi l-programm Ewropa Diġitali għall-perjodu 2021-2027*, COM(2018) 434 final, is-6 ta' Ġunju 2018.

[85] Il-Kummissjoni Ewropea, ir-*Regolament (UE) 2018/1092 tal-Parlament Ewropew u tal-Kunsill tat-18 ta' Lulju 2018 li jistabbilixxi l-Programm Ewropew għall-Iżvilupp fl-Industrija tad-Difiża bil-għan li jappoġġa l-kompetittività u l-kapaċità ta' innovazzjoni tal-industrija tad-difiża tal-Unjoni* (ĠU L 200, 7.8.2018, p. 30). Barra minn hekk, fl-2017, ġiet stabbilita azzjoni preparatorja rigward ir-riċerka dwar id-difiża, li tammonta għal total ta' EUR 90 miljun għall-perjodu 2017-2019 u ffinanzjata minn H2020, ġiet stabbilita fl-2017. Mhuwiex ċar jekk din tinkludix infiq relatat mal-qasam ċibernetiku.

[86] Dokument informattiv u analitiku separat, mill-QEA, dwar id-difiża tal-UE huwa ppjanat li jiġi ppubblikat fl-2019.

[87] L-EC3 tal-Europol, l-ENISA, is-SEAE, l-Aġenzija Ewropea għad-Difiża u s-CERT-UE għandhom forza tax-xogħol ikkombinata ta' 159 membru tal-persunal. Dan it-total ma jinkludix persunal relatat mal-qasam ċibernetiku fil-Kummissjoni Ewropea jew fl-Istati Membri. Sors: Iċ-Ċentru għall-Istudji Politiċi Ewropej, *ibid.*, Novembru 2018.

[88] *ENISA evaluation* (Evalwazzjoni tal-ENISA), 2017.

[89] Fil-Pjan Pluiennali 2018-2020 tagħha, l-Europol talbet żieda annwali ta' 70 aġent temporanju fil-persunal, iżda għall-2018 ġiet approvata żieda ta' 26 aġent biss. Fl-abbozz ta' pjan pluriennali li jmiss għall-perjodu 2019-2021, l-Europol ikkunsidrat żieda modesta, bis-suppożizzjoni li domanda akbar għal riżorsi mhix se tiġi ssodisfata. Sors: Il-Konsultazzjoni dwar l-abbozz ta' Programmazzjoni Pluriennali 2019-2021, li ġiet ippreżentata lill-Grupp ta' Skrutinju Parlamentari Konġunt, A 000834, l-1 ta'Frar 2018.

[90] *ENISA evaluation* (Evalwazzjoni tal-ENISA), 2017. Bejn l-2014 u l-2016, madwar 80 % tal-baġit operazzjonali tal-ENISA ntuża għall-akkwist ta' studji.

[91] L-ENISA, *Exploring the opportunities and limitations of current Threat Intelligence Platforms* (Esplorazzjoni tal-opportunitajiet u l-limitazzjonijiet ta’ Pjattaformi attwali tal-Intelligence dwar it-Theddid), Diċembru 2017.

[92] L-ISACA (preċedentement magħrufa bħala l-Assoċjazzjoni għall-Awditjar u l-Kontroll tas-Sistemi tal-Informazzjoni, *Information Security Governance: Guidance for Boards of Directors and Executive Management* (Governanza tas-Sigurtà tal-Informazzjoni: Gwida għall-Bordijiet tad-Diretturi u l-Maniġment Eżekuttiv), it-tieni ed., 2006.

[93] L-EY, *Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017* (Ksib lura taċ-Ċibersigurtà: tħejjija biex jiġu ffaċċjati ċ-ċiberattakki. L-20 Stħarriġ Globali tal-2017 dwar is-Sigurtà tal-Informazzjoni), p. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy u H. Lung), *Hit or myth? Understanding the true costs and impact of cybersecurity programs* (Veru jew le? Fehim tal-ispejjeż u l-impatt veri ta’ programmi taċ-ċibersigurtà), Lulju 2017.

[95] Il-Kummissjoni għat-Titoli u l-Kambju, *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures* (Dikjarazzjoni u Gwida Interpretattiva dwar id-Divulgazzjonijiet taċ-Ċibersigurtà ta’ Kumpaniji Pubbliċi), il-21 ta’ Frar 2018.

[96] Forum għall-kooperazzjoni bejn l-Awtorità Bankarja Ewropea, l-Awtorità Ewropea tat-Titoli u s-Swieq u l-Awtorità Ewropea tal-Assigurazzjoni u l-Pensjonijiet tax-Xogħol.

[97] L-Awtorità Ewropea tat-Titoli u s-Swieq, *Joint Committee report on risks and vulnerabilities in the EU financial system* (Rapport tal-Kumitat Konġunt dwar ir-riskji u l-vulnerabbiltajiet fis-sistema finanzjarja tal-UE), April 2018.

[98] L-ENISA, *Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs* (Sigurtà tal-informazzjoni u standards tal-privatezza għall-SMEs: Rakkomandazzjonijiet għal titjib fl-adozzjoni tas-sigurtà tal-informazzjoni u l-istandards tal-privatezza fl-SMEs), Diċembru 2015.

[99] B’referenza għall-Istati Membri tal-UE, il-Mekkaniżmu għall-Pariri Xjentifiċi tal-Kummissjoni osserva l-livell sostanzjali u uniku ta’ ftehim dwar il-prinċipji u l-valuri fundamentali, kif ukoll interess strateġiku kondiviż li jista’ jkun fil-qalba ta’ governanza effettiva taċ-ċibersigurtà tal-UE. Sors: L-Opinjoni Xjentifika Nru 2/2017, l-24 ta’ Marzu 2017.

[100] L-Istati Uniti, iċ-Ċina, il-Ġappun, il-Korea t'Isfel, l-Indja u l-Brażil.

[101] Il-Kulleġġ Ewropew ta' Sigurtà u ta' Difiża (T. Renard u A. Barrinha), *Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence* (Manwal dwar iċ-ċibersigurtà, il-Kapitolu 3.4 L-UE bħala sieħeb fiċ-ċiberdiplomazija u ċ-ċiberdifiża), it-23 ta’ Novembru 2018.

[102] Il-Kunsill tal-Unjoni Ewropea, *Pjan ta' Azzjoni għall-implimentazzjoni tal-Konklużjonijiet tal-Kunsill dwar il-Komunikazzjoni Konġunta lill-Parlament Ewropew u lill-Kunsill: Reżiljenza, Deterrenza u Difiża: Il-bini ta' ċibersigurtà b'saħħitha għall-UE*, 15748/17, it-12 ta’ Diċembru 2017.

[103] Il-Kummissjoni Ewropea, *European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission* (Strateġija Diġitali tal-Kummissjoni Ewropea: Kummissjoni trasformata diġitalment, iffukata fuq l-utenti u xprunata mid-*data*), C(2018) 7118 final, il-21 ta' Novembru 2018.

[104] Ir-risposta tal-Kummissarju Gabriel għall-mistoqsija parlamentari bil-miktub (E-004294-17), it-28 ta' Ġunju 2017.

[105] Il-Kunsill tal-Unjoni Ewropea, *Annual Report on the Implementation of the Cyber Defence Policy Framework* (Rapport Annwali dwar l-Implimentazzjoni tal-Qafas ta' Politika dwar iċ-Ċiberdifiża), 15870/17, id-19 ta' Diċembru 2017.

[106] Id-Deċiżjonijiet 2015/443, 2015/444 u 2017/46 jirregolaw is-sigurtà tas-sistemi ta' komunikazzjoni u informazzjoni tal-Kummissjoni. Id-Deċiżjoni tal-Kummissjoni C(2018) 7706 tal-21 ta' Novembru 2018 tistabbilixxi Bord tat-Teknoloġija tal-Informazzjoni u taċ-Ċibersigurtà, li jgħaqqad flimkien il-Bord tal-IT preċedenti u l-Bord ta' Tmexxija tas-Sigurtà tal-Informazzjoni.

[107] Il-Kumitat Ekonomiku u Soċjali Ewropew, *ibid.*, Marzu 2018.

[108] Il-Parlament Ewropew, *ibid.*, Settembru 2015.

[109] Iċ-Ċellola ta' Fużjoni kontra t-Theddid Ibridu ġiet stabbilita fl-2016 fi ħdan iċ-Ċentru tal-Intelligence u tas-Sitwazzjonijiet tal-UE tas-SEAE. Hija tirċievi u tanalizza informazzjoni kklassifikata u minn sorsi miftuħa mingħand partijiet ikkonċernati differenti li jirrigwardaw it-theddid ibridu.

[110] L-ENISA, *National-level Risk Assessments: An Analysis Report* (Valutazzjonijiet tar-Riskju fil-Livell nazzjonali: Rapport ta' Analiżi), Novembru 2013.

[111] Il-Kummissjoni Ewropea, *Impact assessment on the EU Cybersecurity Agency and Cybersecurity Act* (Valutazzjoni tal-impatt dwar l-Aġenzija tal-UE għaċ-Ċibersigurtà u l-Att dwar iċ-Ċibersigurtà), SWD(2017) 500 final (il-Parti 1/6), it-13 ta' Settembru 2017.

[112] Il-Kummissjoni Ewropea, *ibid.*, SWD(2018) 403 final, it-12 ta' Settembru 2018.

[113] Résaux IP Européens Network Coordination Centre, ir-reġistru reġjonali tal-internet għall-Ewropa, li jissorvelja l-allokazzjoni u r-reġistrazzjoni tar-riżorsi tan-numri tar-reġistru tal-internet.

[114] L-ENISA, *EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs* (Żieda tas-Sensibilizzazzjoni Kollaborattiva u Pilota fuq Skala Kbira dwar l-EISAS għaċ-Ċittadini u l-SMEs tal-UE), Novembru 2012.

[115] Iċ-Ċentru għas-Sikurezza u l-Edukazzjoni fil-qasam taċ-Ċibersigurtà, fi sħubija ma' Booz Allen Hamilton, Alta Associates u Frost & Sullivan, *2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk* (Studju tal-2017 dwar il-Forza tax-Xogħol Globali relatata mas-Sigurtà tal-Informazzjoni – Valutazzjoni komparattiva tal-Kapaċità tal-Forza tax-xogħol u r-Rispons għar-Riskju Ċibernetiku).

[116] Il-Kumitat Ekonomiku u Soċjali Ewropew, *ibid.*, Marzu 2018.

[117] Il-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* (Il-Kumitat Konġunt tal-House of Commons dwar l-Istrateġija tas-Sigurtà Nazzjonali, il-Ħiliet fil-qasam taċ-Ċibersigurtà u l-Infrastruttura Nazzjonali Kritika tar-Renju Unit, it-Tieni Rapport tas-Sessjoni 2017–19), is-16 ta' Lulju 2018.

[118] L-Europol/l-Eurojust, *Common challenges in combatting cybercrime* (Sfidi komuni fil-ġlieda kontra ċ-ċiberkriminalità), 7021/17, it-13 ta' Marzu 2017.

[119] L-Europol/l-Eurojust, *ibid.*, 7021/17, it-13 ta' Marzu 2017.

[120] Il-Kummissjoni Ewropea, *ibid.*, SWD(2018) 403 final, it-12 ta' Settembru 2018.

[121] Is-CEPOL, *Decision of the Management Board 33/2018/MB on the CEPOL Single Programming Document 2020-2022* (Deċiżjoni 33/2018/MB tal-Bord Maniġerjali dwar id-Dokument Uniku ta' Programmazzjoni tas-CEPOL għall-perjodu 2020-2022), l-20 ta' Novembru 2018.

[122] Pereżempju, il-kooperazzzjoni bejn is-SEAE, l-Istati Membri, l-aġenziji u l-korpi bħas-CEPOL, l-ECTEG jew l-EDSC.

[123] L-ENISA, *Stock-taking of information security training needs in critical sectors* (Rendikont ta' ħtiġijiet ta' taħriġ relatat mas-sigurtà tal-informazzjoni f'setturi kritiċi), Diċembru 2017.

[124] Il-Grupp Ewropew għat-Taħriġ u l-Edukazzjoni dwar iċ-Ċiberkriminalità.

[125] Il-Kummissjoni Ewropea, It-tlettax-il rapport ta' progress lejn Unjoni tas-Sigurtà effettiva u ġenwina, COM(2018) 46 final, l-24 ta' Jannar 2018.

[126] Ibbażat fuq osservazzjonijiet fir-Rapport Speċjali Nru 14/2018, *ibid.*

[127] Ir-Riżoluzzjoni tal-Parlament Ewropew tat-13 ta' Ġunju 2018 dwar iċ-ċiberdifiża (2018/2004(INI)). Il-Kunsill tal-Unjoni Ewropea, *ibid.*, 15870/17, id-19 ta' Diċembru 2017.

[128] L-iżvizzera, l-Eks-Repubblika Jugoslava tal-Maċedonja, l-Ukrajna, il-Bożnija-Ħerzegovina, il-Kosovo (dan l-isem huwa mingħajr preġudizzju għall-pożizzjonijiet dwar l-istatus, u huwa konformi mal-UNSCR 1244/1999 u l-Opinjoni tal-QIĠ dwar id-dikjarazzjoni tal-indipendenza tal-Kosovo), it-Turkija u l-Istati Uniti.

[129] L-Europol, *Internet Organised Crime Threat Assessment 2018* (Valutazzjoni tal-2018 dwar it-Theddida mill-Kriminalità Organizzata ffaċilitata mill-Internet).

[130] Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta' Settembru 2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman u S. Furman, *Security Fatigue* (Eżawriment minħabba s-Sigurtà), "IT Professional", il-Vol. 18, Nru 5, 2016, pp. 26-32. Ara wkoll l-NIST.

[132] Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *Increasing resilience and bolstering capabilities to address hybrid threats* (Żieda tar-reżiljenza u appoġġ għall-kapaċitajiet biex jiġi indirizzat it-theddid ibridu), JOIN(2018) 16 final, it-13 ta' Ġunju 2018.

[133] Pereżempju, l-għeluq ta' AlphaBay u ta' Hansa f'operazzjonijiet konġunti mmexxija mill-FBI u mill-pulizija nazzjonali Netherlandiża bl-appoġġ tal-Europol. Dawn kienu tnejn mill-akbar swieq għan-negozjar ta' prodotti illeċiti bħal drogi, armi tan-nar u għodod taċ-

ċiberkriminalità, bħal malware. Sors: L-Europol, *Crime on the Dark Web: Law Enforcement coordination is the only cure* (Kriminalità fuq id-Dark Web: Il-koordinazzjoni fost l-awtoritajiet tal-infurzar tal-liġi hija l-unika soluzzjoni), Stqarrija għall-Istampa, id-29 ta’ Mejju 2018.

134 Il-Kummissjoni Ewropea, *ibid.*, SWD(2018) 403 final, it-12 ta’ Settembru 2018.

135 Il-Kunsill tal-Unjoni Ewropea, *ibid.*, 12711/1/17 REV 1, id-9 ta’ Ottubru 2017.

136 Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta’ Settembru 2017.

137 Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *ibid.*, JOIN (2018) 16, it-13 ta’ Ġunju 2018.

138 Il-Kummissjoni Ewropea, SWD(2017) 500 final, it-13 ta’ Settembru 2017.

139 *Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU* (Memorandum ta' Qbil – l-ENISA, l-EDA, l-EC3 tal-Europol, u s-CERT-UE); it-23 ta’ Mejju 2018.

140 Il-Kummissjoni Ewropea, Sejħa għall-offerti: *Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap* (Stabbiliment u operazzjoni ta’ proġett pilota għal Netwerk ta’ Kompetenza dwar iċ-Ċibersigurtà biex jiġi żviluppat u implimentat Pjan Direzzjonali komuni għar-Riċerka u l-Innovazzjoni fil-qasam taċ-Ċibersigurtà), is-27 ta’ Ottubru 2017.

141 Jean-Claude Juncker, Mission letter for the Commissioner for the Security Union (Ittra ta’ missjoni għall-Kummissjarju għall-Unjoni tas-Sigurtà), it-2 ta’ Awwissu 2016. Id-difiża ma taqax taħt ir-responsabbiltà tat-task force.

142 Il-Kunsill tal-Unjoni Ewropea, *EU cybersecurity roadmap* (Pjan direzzjonali tal-UE għaċ-ċibersigurtà), 8901/17, il-11 ta’ Mejju 2017.

143 Friends of Europe, *Debating Security Plus: Crowdsourcing solutions to the world's security issues (Dibattitu dwar is-Security Plus: Soluzzjonijiet ta’ crowdsourcing għall-kwistjonijiet relatati mas-sigurtà fid-dinja); il-ħames ed.*, Novembru 2017.

144 Rapporti Tekniċi tal-JRC, Mappa taċ-Ċentri Ewropej ta’ Għarfien Espert fil-qasam taċ-Ċibersigurtà: *Definizzjonijiet u Tassonomija.* Valutazzjoni tal-impatt dwar il-proposta għal Ċentru ta’ Kompetenza tar-Riċerka u n-Netwerk ta’ Ċentri Nazzjonali ta’ Koordinazzjoni, SWD(2018) 403 final, it-12 ta’ Settembru 2018.

145 Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta’ Settembru 2017.

146 Il-Kummissjoni Ewropea, *ibid.*, SWD(2018) 403 final, it-12 ta’ Settembru 2018.

147 Pereżempju, l-ISAC tal-Istituti Finanzjarji Ewropej jinkludi rappreżentanti tas-settur finanzjarju, CERTs nazzjonali, aġenziji tal-infurzar tal-liġi, l-ENISA, l-Europol, il-Bank Ċentrali Ewropew, il-Kunsill Ewropew għall-Pagamenti u l-Kummissjoni Ewropea.

148 L-ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models* (Mudelli kooperattivi taċ-Ċentri tal-Kondiviżjoni u tal-Analiżi tal-Informazzjoni (ISACs)), l-14 ta’ Frar 2018.

[149] Il-Kunsill tal-Unjoni Ewropea, *ibid.*, 12711/1/17 REV 1, id-9 ta' Ottubru 2017.

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

[151] Studju li sar fl-2018 minn Accenture fi 15-il pajjiż sabu li 87 % taċ-ċiberattakki ffukati kienu qed jiġu pprevenuti: *2018 State of Cyber Resilience* (Stat tar-Reżiljenza Ċibernetika fl-2018), l-10 ta' April 2018.

[152] P. Timmers, *Cybersecurity is Forcing a Rethink of Strategic Autonomy* (Iċ-Ċibersigurtà qed Tikkaġuna Riforma tal-Awtonomija Strateġika), Oxford University Politics Blog, l-14 ta' Settembru 2018.

[153] Caroline Preece, *Three reasons why cyber threat detection is still ineffective* (Tliet raġunijiet għalfejn l-identifikazzjoni ta' theddid ċibernetiku għadu ineffettiv), IT Pro, l-14 ta' Lulju 2017.

[154] Il-Kumitat Ekonomiku u Soċjali Ewropew, *ibid.*, Marzu 2018.

[155] Il-Kummissjoni Ewropea, *It-tmien rapport ta' progress lejn Unjoni tas-Sigurtà effettiva u ġenwina*, COM(2017) 354 final, id-29 ta' Ġunju 2017.

[156] Ara d-diversi pubblikazzjonijiet tal-Grupp ta' Kooperazzjoni NIS.

[157] Il-PSD2: id-Direttiva dwar is-Servizzi ta' Ħlas 2; il-BĊE/l-MSU: il-Bank Ċentrali Ewropew/il-Mekkaniżmu Superviżorju Uniku; Target 2: Is-sistema ta' Trasferiment Fil-pront Awtomatizzat Trans-Ewropew għall-Pagament Gross f'Ħin reali (it-tieni ġenerazzjoni), ir-Regolament (UE) Nru 910/2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal transazzjonijiet elettroniċi fis-suq intern. Sors: It-Task Force tas-CEPS-ECRI, *ibid.*, Ġunju 2018.

[158] Il-Kummissjoni Ewropea, *Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises* (Rakkomandazzjoni dwar ir-Rispons Ikkoordinat għal Inċidenti u Kriżijiet taċ-Ċibersigurtà fuq Skala Kbira), C(2017) 6100 final, it-13 ta' Settembru 2017.

[159] Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta' Settembru 2017. Hemm bosta mekkaniżmi ta' ġestjoni ta' kriżijiet, inkluż il-mekkaniżmu ta' Rispons Politiku Integrat f'Sitwazzjonijiet ta' Kriżi (IPCR), Argus (il-mekkaniżmu ta' rispons għall-kriżijiet tal-Kummissjoni), il-Mekkaniżmu ta' Rispons għall-Kriżijiet tas-SEAE, il-Mekkaniżmu tal-Unjoni għall-Protezzjoni Ċivili u l-Protokoll ta' Rispons ta' Emerġenza għall-Infurzar tal-Liġi tal-UE.

[160] Barra minn hekk, dan jista' jwassal ukoll biex jiġi invokat l-Artikolu 42(7) tat-Trattat dwar il-Funzjonament tal-Unjoni Ewropea (klawżola ta' assistenza reċiproka) jew l-Artikolu 222 tat-Trattat dwar il-Funzjonament tal-Unjoni Ewropea (klawżola ta' solidarjetà).

[161] Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *ibid.* JOIN(2018) 16, it-13 ta' Ġunju 2018. F'Diċembru 2018, ġew irrappurtati fil-midja hacks allegati tan-netwerk diplomatiku ta' komunikazzjoni tas-SEAE, COREU (sors: *New York Times, Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran* (New York Times, Kejbils Ewropej Aċċessati b'mod illegali Jiżvelaw Dinja ta' Ansjetà dwar Trump, ir-Russja u l-Iran); it-18 ta' Diċembru 2018). Attwalment, il-kwistjoni qed tiġi investigata.

[162] Jeħtieġ li l-kooperazzjoni dwar it-twissijiet bikrija u l-assistenza reċiproka wkoll tkompli tiġi żviluppata: *Council Conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises* (Konklużjonijiet tal-Kunsill dwar ir-Rispons Ikkoordinat tal-UE għal Inċidenti u Kriżijiet taċ-Ċibersigurtà fuq Skala Kbira), 10085/18, is-26 ta' Ġunju 2018.

[163] Is-Servizz ta' Riċerka tal-Parlament Ewropew, *Briefing EU Legislation in Progress: ENISA and a new cybersecurity act* (Tgħarrif: Leġiżlazzjoni tal-UE li għadha qed titfassal: l-ENISA u att ġdid dwar iċ-ċibersigurtà), PE 614.643, Settembru 2018.

[164] Il-Kumitat Ekonomiku u Soċjali Ewropew, *ibid.*, Marzu 2018.

[165] Il-Kunsill tal-Unjoni Ewropea, *EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks* (Il-Protokoll ta' Rispons ta' Emerġenza għall-Infurzar tal-Liġi tal-UE (LE ERP)), 14893/18, Diċembru 2018.

[166] Timijiet ta' Rispons Rapidu Ċibernetiku u Assistenza Reċiproka fil-Qasam taċ-Ċibersigurtà; Pjattaforma għall-Kondiviżjoni tal-Informazzjoni dwar it-Theddid Ċibernetiku u r-Rispons għall-Inċidenti. Sors: Il-Kunsill tal-Unjoni Ewropea, *Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview* (Kooperazzjoni Strutturata Permanenti (PESCO) - Lista aġġornata ta' proġetti tal-PESCO – Stampa ġenerali), id-19 ta' Novembru 2018.

[167] Il-Kunsill tal-Unjoni Ewropea, Konklużjonijiet dwar Qafas għal Rispons Diplomatiku Konġunt tal-UE għal Attivitajiet Ċibernetiċi Malizzjużi, 9916/17, is-7 ta' Ġunju 2017.

[168] Il-Kunsill tal-Unjoni Ewropea, *Konklużjonijiet tal-Kunsill dwar iċ-Ċiberdiplomazija*, 6122/55, il-11 ta' Frar 2015.

[169] Il-Kunsill tal-Unjoni Ewropea, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities* (Abbozz ta' linji gwida ta' implimentazzjoni għall-Qafas dwar Rispons Diplomatiku Konġunt għal Attivitajiet Ċibernetiċi Malizzjużi), 13007/17.

[170] L-attribuzzjoni ta' responsabbiltà għal inċident tibqa' deċiżjoni politika sovrana għall-Istati Membri, u mhux il-miżuri kollha tas-sett ta' għodod jirrikjedu attribuzzjoni.

[171] Is-sett ta' għodod ma wassalx għal azzjoni konġunta; Stati Membri individwali adottaw il-pożizzjoni tal-Istati Uniti.

[172] Il-Kunsill tal-Unjoni Ewropea, *Konklużjonijiet dwar attivitajiet ċibernetiċi malizzjużi*, 7925/18, is-16 ta' April 2018.

[173] Sistemi tal-kompjuter użati għall-kontroll ta' proċessi f'diversi industriji, bħal utilitajiet, manifattura industrijali u ta' sustanzi kimiċi, ipproċessar tal-ikel, sistemi tat-trasport u hubs, kif ukoll servizzi loġistiċi.

[174] L-ENISA, *ibid.*, Diċembru 2017.

[175] Pereżempju, l-amministrazzjoni pubblika, industrija tal-kimika u dik nukleari, il-manifattura, l-ipproċessar tal-ikel, it-turiżmu, il-loġistika u l-protezzjoni ċivili.

[176] Il-Kummissjoni Ewropea, *ibid.*, SWD(2017) 295 final, it-13 ta' Settembru 2017.

[177] Diskors mill-Kummissarju Jourová fis-Sessjoni Plenarja tal-Parlament Ewropew dwar *Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign* (iż-żieda tar-reżiljenza tal-UE kontra l-influwenza ta’ atturi barranin fuq il-kampanja elettorali tal-PE li jmiss), l-14 ta’ Novembru 2018.

[178] Carnegie Endowment for International Peace, *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks* (Interferenza fl-Elezzjoni tar-Russja: il-Ġlieda tal-Ewropa Kontra l-Aħbarijiet Foloz u ċ-Ċiberattakki), it-23 ta’ Mejju 2018.

[179] Iċ-Ċentru Ewropew ta' Strateġija Politika (L. Past), Ċibersigurtà tat-Teknoloġija Elettorali: Attakki Inevitabbli u Varjetà ta’ Reazzjonijiet, f’: “Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts” (Interferenza Elettorali fl-Era Diġitali – Tisħiħ tar-Reżiljenza għal Theddid bl-Użu tal-Internet: Ġabra ta’ noti ta' riflessjoni minn 35 professjonist u esperti ewlenin), 2018.

[180] Skont id-Direttiva tal-Kunsill 2008/114/KE dwar l-identifikazzjoni u l-indikazzjoni tal-Infrastruttura Kritika Ewropea u l-valutazzjoni tal-ħtieġa għat-titjib tal-ħarsien tagħhom.

[181] Il-Kummissjoni Ewropea, Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament (Rakkomandazzjoni dwar in-netwerks ta’ kooperazzjoni fl-elezzjonijiet, it-trasparenza online, il-protezzjoni kontra inċidenti relatati maċ-ċibersigurtà u l-ġlieda kontra kampanji ta’ diżinformazzjoni fil-kuntest ta’ elezzjonijiet għall-Parlament Ewropew), C(2018) 5949 final, it-12 ta’ Settembru 2018.

[182] Il-Konklużjonijiet tal-Kunsill Ewropew, EUCO 11/15, l-20 ta’ Marzu 2015. Minn dak iż-żmien 'il hawn inżdiedu żewġ Task Forces addizzjonali, għall-Balkani tal-Punent u għall-Viċinat tan-Nofsinhar.

[183] Rapport tal-Kunsill tal-Atlantiku appella lill-UE biex tirrikjedi lill-Istati Membri jibagħtu esperti nazzjonali għat-Task Force. Ara: D. Fried u A. Polyakova, *Democratic Defense Against Disinformation* (Difiża Demokratika Kontra d-Diżinformazzjoni), il-5 ta’ Marzu 2018.

[184] Oriġinarjament nieqsa mill-baġit proprju tagħha, fl-2018 ingħatat EUR 1.1 miljun għal Azzjoni Preparatorja “StratCom Plus” mill-Parlament Ewropew.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), *ibid.*, it-23 ta’ Mejju 2018.

[186] Il-Kummissjoni Ewropea, Rappreżentant Għoli tal-Unjoni għall-Affarijiet Barranin u l-Politika ta' Sigurtà, *Action Plan against Disinformation* (Pjan ta’ Azzjoni kontra d-Diżinformazzjoni), JOIN(2018) 36 final. Il-pjan jiffoka fuq: it-titjib tal-kapaċitajiet tal-istituzzjonijiet tal-UE biex jidentifikaw, janalizzaw u jesponu diżinformazzjoni; it-tisħiħ ta’ rispons ikkoordinat u konġunt; il-mobilizzazzjoni tas-settur privat; kif ukoll iż-żieda tas-sensibilizzazzjoni u t-titjib tar-reżiljenza tas-soċjetà.

[187] Il-Kummissjoni Ewropea, *L-indirizzar tad-diżinformazzjoni online: Approċċ Ewropew*, COM(2018) 236 final, is-26 ta’ April 2018.

[188] Ma għandux jiġi konfuż mal-kodiċi ta' kondotta għall-ġlieda kontra d-diskors ta' mibegħda illegali online.

[189] Il-JRC, *The digital transformation of news media and the rise of disinformation and fake news* (It-trasformazzjoni diġitali tal-mezzi tax-xandir u ż-żieda tad-diżinformazzjoni u l-aħbarijiet foloz), Rapporti Tekniċi tal-JRC, Dokument ta' Ħidma dwar l-Ekonomija Diġitali 2018-02 tal-JRC, April 2018.

[190] L-ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")* (Tisħiħ tas-Sigurtà tan-Netwerks u tal-Informazzjoni u l-Protezzjoni Kontra d-Diżinformazzjoni Online ("Fake News")), April 2018.

[191] Iċ-Ċentru Ewropew ta' Strateġija Politika (L. Past), *A Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats* (Responsabbiltà għall-Appoġġ lil Organizzazzjonijiet Elettorali fl-Antiċipazzjoni u l-Ġlieda Kontra t-Theddid Ċibernetiku), f': *ibid*, 2018.

[192] Il-Kummissjoni Ewropea, *ibid.*, SWD(2018) 403 final, it-12 ta' Settembru 2018.

[193] Ir-Regolament propost (COM(2017) 487 final, it-13 ta' Settembru 2018) għall-iskrinjar tal-FDI, li ġie ppreżentat f'Settembru 2017, attwalment qed jgħaddi mill-proċess leġiżlattiv. Huwa speċifikament ikopri teknoloġiji kritiċi, li jinkludu l-intelliġenza artifiċjali, iċ-ċibersigurtà u applikazzjoni b'użu doppju.

[194] Il-Kummissjoni Ewropea/is-Servizz Ewropew għall-Azzjoni Esterna, *ibid.*, JOIN(2017) 450 final, it-13 ta' Settembru 2017.

Tim tal-QEA

Dan id-Dokument Informattiv u Analitiku – *Sfidi għal politika effettiva tal-UE fil-qasam taċ-ċibersigurtà* ġie adottat mill-Awla III, Azzjoni esterna/Sigurtà u ġustizzja, li hija mmexxija minn Bettina Jakobsen, Membru tal-QEA. Il-kompitu tmexxa minn Baudilio Tomé Muguruza, Membru tal-QEA, li ngħata appoġġ minn Daniel Costa de Magalhaes, Kap tal-Kabinett u Ignacio Garcia de Parada, Attaché tal-Kabinett; Alejandro Ballester-Gallardo, Maniġer Prinċipali; Michiel Sweerts, Kap tal-Kompitu; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha, awdituri u Johannes Bolkart, trainee. Hannah Critoph ipprovdiet appoġġ lingwistiku.

Mix-xellug għal-lemin: 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.

IL-QORTI EWROPEA TAL-AWDITURI

L-Uffiċċju tal-Pubblikazzjonijiet

IL-QORTI EWROPEA TAL-AWDITURI
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Mistoqsijiet: eca.europa.eu/mt/Pages/ContactForm.aspx
Sit web: eca.europa.eu
Twitter: @EUAuditors

© L-Unjoni Ewropea, 2019.
Għal kull użu jew riproduzzjoni ta’ ritratti jew materjal ieħor li ma jaqax taħt id-drittijiet tal-awtur tal-Unjoni Ewropea, bħal pereżempju l-logos fil-Figura 4, kif ukoll fl-Annessi I u II, irid jintalab il-permess direttament mingħand id-detenturi tad-drittijiet tal-awtur.
Paġna ta' quddiem: © Syda Productions / Shutterstock.com