IL-KUMMISSJONI EWROPEA

IR-RAPPREŻENTANT GĦOLI TAL-UNJONI GĦALL-AFFARIJIET BARRANIN U L-POLITIKA TA' SIGURTÀ

Brussell, 13.9.2017
JOIN(2017) 450 final

KOMUNIKAZZJONI KONĠUNTA LILL-PARLAMENT EWROPEW U LILL-KUNSILL

Reżiljenza, Deterrenza u Difiża: Il-Bini ta' ċibersigurtà bsaħħitha għall-UE

1. INTRODUZZJONI

Iċ-ċibersigurtà hija essenzjali kemm għall-prosperità kif ukoll għas-sigurtà tagħna. Hekk kif il-ħajja tagħna ta' kuljum u l-ekonomiji tagħna jsiru dejjem aktar dipendenti fuq teknoloġiji diġitali, aħna nsiru dejjem aktar esposti. L-inċidenti taċ-ċibersigurtà qed jiddiversifikaw, kemm f'termini ta' min hu responsabbli kif ukoll f'termini ta' dak li jfittxu li jiksbu. Attivitajiet Ċibernetiċi Malizzjużi ma jheddux biss l-ekonomiji tagħna u l-ispinta lis-Suq Uniku Diġitali, iżda wkoll il-funzjonament innifsu tad-demokraziji, il-libertajiet u l-valuri tagħna. Is-sigurtà tagħna fil-futur tiddependi fuq li nittrasformaw il-kapaċità tagħna li nipproteġu l-UE kontra t-theddid ċibernetiku: Kemm il-kapaċità tal-infrastruttura ċivili kif ukoll il-kapaċità ta' dik militari jserrħu fuq is-sistemi diġitali. Dan ġie rikonoxxut mill-Kunsill Ewropew ta' Ġunju 2017[1], kif ukoll fl-Istrateġija Globali dwar il-Politika Barranija u ta' Sigurtà Komuni għall-Unjoni Ewropea[2].

Ir-riskji qed jiżdiedu b'mod esponenzjali. L-istudji jissuġġerixxu li l-impatt ekonomiku taċ-ċiberkriminalità żdied b'ħames darbiet mill-2013 sal-2017 u jista' jiżdied b'erba' darbiet oħra sal-2019[3]. Ir-ransomware[4] kellu żieda partikolari, bl-attakki riċenti[5] jirriflettu żieda drammatika fl-attività ċiberkriminali. Madankollu, ir-ransomware mhuwiex l-unika theddida.

It-theddid ċibernetiku kien ġej kemm minn atturi mhux statali kif ukoll minn atturi statali: dawn spiss ikunu kriminali, immotivati mill-qliegħ, iżda jistgħu jkunu wkoll politiċi u strateġiċi. It-theddida kriminali hija intensifikata mit-titpin tal-limiti bejn ċiberkriminalità u kriminalità "tradizzjonali", minħabba li l-kriminali jużaw l-internet kemm biex jespandu l-attivitajiet tagħhom, kif ukoll bħala sors biex isibu metodi u għodod ġodda biex iwettqu l-kriminalità[6]. Madankollu, fil-maġġoranza tal-każi, il-probabbiltà li jiġi identifikat il-kriminali huma minimi, u l-probabbiltà ta' prosekuzzjoni huma iżgħar minn hekk.

Fl-istess ħin, l-atturi statali qegħdin dejjem aktar jilħqu l-għanijiet ġeopolitiċi tagħhom mhux biss permezz ta' għodod tradizzjonali bħall-forza militari, iżda permezz ta' għodod ċibernetiċi aktar diskreti, inkluż permezz tal-interferenza fil-proċessi demokratiċi interni. Illum l-użu taċ-ċiberspazju bħala qasam ta' gwerra, kemm waħdu kif ukoll bħala parti mill-approċċ ibridu huwa rikonoxxut b'mod wiesa'. Kampanji ta' diżinformazzjoni, aħbarijiet foloz u operazzjonijiet ċibernetiċi mmirati lejn infrastruttura kritika qed isiru aktar komuni u jeħtieġu rispons. Għal din ir-raġuni, fil-Karta ta' Riflessjoni tagħha dwar il-Ġejjieni tad-Difiża Ewropea[7] il-Kummissjoni enfasizzat l-importanza ta' kooperazzjoni fid-difiża ċibernetika.

Sakemm ma ntejbux b'mod sostanzjali ċ-ċibersigurtà tagħna, ir-riskju se jiżdied mat-trasformazzjoni diġitali. Sal-2020, għexieren ta' biljuni ta' apparat ta' "Internet tal-Oġġetti" huma mistennija jkunu konnessi mal-internet, iżda ċ-ċibersigurtà għad mhijiex prijoritizzata fid-disinn tagħhom [8]. Fin-nuqqas li jiġu protetti l-apparati li jikkontrollaw il-grilji tal-enerġija

---

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

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

3 Ara pereżempju McAfee & Centre for Strategic and International Studies "Net losses: Estimating the Global Cost of Cybercrime" 2014.

4 Ir-ransomware huwa tip ta' softwer malizzjuż li jipprevjeni jew jillimita lill-utenti li jaċċessaw is-sistema tagħhom, jew billi jimblokka l-iskrin tas-sistema inkella billi jimblokka l-fajls tal-utenti sakemm titħallas somma flus.

5 F'Mejju 2017 l-attakk ta' ransomware WannaCry affettwa aktar minn 400,000 kompjuter f'aktar minn 150 pajjiż. Xahar wara, l-attakk ta' ransomware "Petya" laqat lill-Ukrajna u lil diversi kumpaniji madwar id-dinja.

6 EUROPOL, Valutazzjoni ta' Theddid mill-Kriminalità Organizzata 2017.

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

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, studju għall-Kummissjoni.

tagħna, il-karozzi u n-netwerks tat-trasport, il-fabbriki, il-finanzi, l-isptarijiet u d-djar jista' jkollhom konsegwenzi devastanti u jikkawżaw ħsara kbira għall-fiduċja tal-konsumatur f'teknoloġiji emerġenti. Ir-riskju ta' attakki politikament motivati fuq miri ċivili u ta' nuqqasijiet fil-qasam tad-difiża ċibernetika ikompli japprofondixxi r-riskju aktar.

L-approċċ stabbilit f'din il-Komunikazzjoni Konġunta se jagħmel l-UE f'pożizzjoni aħjar biex taffaċċja dawn it-theddidiet. Dan jibni reżiljenza akbar u awtonomija strateġika, u jżid il-kapaċitajiet f'termini ta' teknoloġija u ħiliet, kif ukoll jgħin li jinbena suq uniku b'saħħtu. Għal dan hemm bżonn li l-istrutturi t-tajba jkunu fis-seħħ biex tinbena ċibersigurtà b'saħħitha u jkun hemm reazzjoni malli tkun meħtieġa, bl-involviment sħiħ tal-atturi ewlenin kollha. L-approċċ jiskoraġġixxi b'mod aħjar ukoll l-attakki ċibernetiċi, billi jżid il-ħidma biex jiġu identifikati, traċċati u miżmuma dawk responsabbli. Dan jagħraf ukoll id-dimensjoni globali milli jiżviluppa kooperazzjoni internazzjonali bħala pjattaforma għat-tmexxija tal-UE dwar iċ-ċibersigurtà. Dawn il-passi jibnu fuq l-approċċi tas-Suq Uniku Diġitali, l-Istrateġija Globali, l-Aġenda Ewropea dwar is-Sigurtà[9], il-Qafas Konġunt dwar il-ġlieda kontra t-theddid ibridu [10] u l-Komunikazzjoni dwar it-Tnedija ta' Fond Ewropew għad-Difiża[11][12].

L-UE diġa' qed taħdem fuq ħafna minn dawn il-kwistjonijiet: wasal iż-żmien li l-flussi ta' ħidma differenti jingħaqdu flimkien. Fl-2013, L-UE waqqfet Strateġija taċ-Ċibersigurtà li tniedi serje ta' flussi tax-xogħol ewlenin biex ittejjeb ir-reżiljenza ċibernetika[13]. L-għanijiet u l-prinċipji ewlenin tagħha li trawwem ekosistema ċibernetika affidabbli, sigura u miftuħa jibqgħu validi. Iżda l-evolviment tax-xenarju ta' theddida dejjem jevolvi u kontinwu jitlob għal aktar azzjoni biex fil-futur ikun hemm aktar reżistenza għall-attakki jew jiġu skoraġġuti[14].

L-UE tinsab f'pożizzjoni tajba biex tindirizza ċ-ċibersigurtà, minħabba l-kamp ta' applikazzjoni tal-politiki tagħha u l-għodod, l-istrutturi u l-kapaċitajiet disponibbli għaliha. Filwaqt li l-Istati Membri jibqgħu responsabbli għas-sigurtà nazzjonali, l-iskala u n-natura transfruntiera tat-theddida huma biżżejjed biex l-UE tieħu azzjoni li tipprovdi inċentivi u tappoġġja lill-Istati Membri biex tiżviluppa u żżomm aktar kapaċitajiet taċ-ċibersigurtà nazzjonali u kapaċitajiet aħjar, filwaqt li fl-istess ħin tibni l-kapaċità fil-livell tal-UE. Dan l-approċċ huwa mfassal biex jistimula l-atturi kollha - lill-UE, lill-Istati Membri, lill-industriji u lill-individwi - biex jagħti liċ-ċibersigurtà l-prijorità li għandha bżonn biex tibni r-reżiljenza u jkollha rispons aħjar fil-livell tal-UE għal attakki ċibernetiċi. Dan se jġib passi konkreti biex jgħin jagħraf u jinvestiga kwalunkwe forma ta' inċidenti ċibernetiċi kontra l-UE u l-Istati Membri tagħha u biex jirreaġixxi b'mod xieraq, inkluż permezz tal-prosekuzzjoni tal-kriminali. Dan se jippermetti li l-azzjoni esterna tal-UE tippromwovi b'mod effettiv iċ-ċibersigurtà fuq livell globali. Ir-riżultat se jkun ċaqliqa għall-UE minn approċċ reattiv għal approċċ proattiv biex jipproteġi l-ħarsien tal-prosperità tal-Ewropa, is-soċjetà u l-valuri, kif ukoll id-drittijiet u l-libertajiet fundamentali, permezz ta' rispons kemm għal theddid eżistenti kif ukoll għal dak futur.

---

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295 final.

12 L-approċċ huwa sostnut ukoll permezz ta' parir xjentifiku indipendenti mogħti mill-Grupp ta' Livell Għoli ta' Konsulenti Xjentifiċi tal-Mekkaniżmu għall-Parir Xjentifiku tal-Kummissjoni Ewropea (ara r-referenzi hawn taħt).

13 JOIN(2013) 1 final. Valutazzjoni ta' din l-istrateġija hija disponibbli fl-SWD (2017) 295.

14 Sakemm ma jkunx iddikjarat mod ieħor, il-proposti f'din il-Komunikazzjoni huma newtrali għall-finijiet ta' baġit. Kwalunkwe inizjattiva li għandha implikazzjonijiet baġitarji se ssegwi l-proċeduri baġitarji annwali u ma tistax tippreġudika l-Qafas Finanzjarju Pluriennali li jmiss ta' wara l-2020.

2. NIBNU R-REŻILJENZA TAL-UE GĦAL ATTAKKI ĊIBERNETIĊI

Reżiljenza ċibernetika b'saħħitha għandha bżonn ta' approċċ wiesa' u kollettiv. Dan jitlob għal strutturi aktar robusti u effettivi biex jippromwovu ċ-ċibersigurtà u biex iwieġbu għal attakki ċibernetiċi fl-Istati Membri iżda wkoll l-istituzzjonijiet, l-aġenziji u l-korpi stess tal-UE. Dan jirrikjedi wkoll approċċ aktar komprensiv, approċċ trans-politiku għall-bini ta' reżiljenza ċibernetika u awtonomija strateġika, b'Suq Uniku b'saħħtu, avvanzi kbar fil-kapaċità teknoloġika tal-UE, u numru ferm akbar ta' esperti b'livell għoli ta' ħiliet. Fil-qalba ta' dan hemm aċċettazzjoni usa' li ċ-ċibersigurtà hija sfida komuni tas-soċjetà, biex b'hekk ikunu involuti għadd ta' livelli differenti ta' gvern, ekonomija u s-soċjetà.

2.1 It-tisħiħ tal-Aġenzija tal-Unjoni Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni

L-**Aġenzija tal-Unjoni Ewropea dwar is-Sigurtà tan-Netwerks u l-Informazzjoni (**ENISA) għandha rwol ewlieni fit-tisħiħ tar-reżiljenza ċibernetika tal-UE u r-rispons tagħha iżda hija ristretta skont il-mandat attwali tagħha. Il-Kummissjoni, għalhekk, qed tressaq proposta ta' riforma ambizzjuża, **inkluż mandat permanenti għall-aġenzija**[15]. Dan se jiżgura li l-ENISA tipprovdi appoġġ lill-Istati Membri, l-istituzzjonijiet tal-UE u n-negozji f'oqsma ewlenin, inkluża l-implimentazzjoni tad-Direttiva dwar is-Sigurtà tan-Netwerks u tas-Sistemi tal-Informazzjoni[16] ("id-Direttiva NIS") u l-Qafas ta' ċertifikazzjoni taċ-ċibersigurtà propost.

L-ENISA riformata se jkollha rwol ta' konsulenza b'saħħtu fuq l-iżvilupp tal-politika u l-implimentazzjoni, inkluż il-promozzjoni tal-koerenza bejn inizjattivi settorjali u d-Direttiva dwar iċ-Ċibersigurtà (NIS) kif ukoll fl-għajnuna fit-twaqqif ta' Ċentri Settorjali għall-Kondiviżjoni tal-Informazzjoni f'setturi kritiċi. L-ENISA se ttejjeb il-livell u żżid it-tħejjija Ewropea billi torganizza eżerċizzji ċibernetiċi pan-Ewropej kull sena li jgħaqqdu r-rispons fuq livelli differenti. Hija ser tappoġġja wkoll żvilupp tal-politika tal-UE dwar iċ-ċertifikazzjoni ċibernetika tat-teknoloġija tal-informazzjoni u tal-komunikazzjoni (ICT) u ser ikollha rwol importanti biex jiżdiedu kemm il-kooperazzjoni operazzjonali kif ukoll l-immaniġġar ta' kriżijiet madwar l-UE. L-aġenzija se sservi wkoll bħala punt fokali ta' informazzjoni u għarfien fil-komunità taċ-ċibersigurtà.

Fehim rapidu u kondiviż dwar it-theddid u l-inċidenti kif iseħħu huwa prerekwiżit biex jiġi deċiż jekk hijiex meħtieġa azzjoni ta' mitigazzjoni konġunta jew rispons appoġġjat mill-UE. Skambju ta' informazzjoni bħal dan jirrikjedi l-involviment tal-atturi rilevanti kollha — il-korpi u l-aġenziji tal-UE, kif ukoll l-Istati Membri — f'livell tekniku, operazzjonali u strateġiku. L-ENISA, f'kooperazzjoni mal-korpi rilevanti fil-livell tal-Istati Membri u fil-livell tal-UE, b'mod partikolari man-Netwerk tal-iskwadri ta' rispons għal inċidenti relatati mas-sigurtà tal-kompjuters[17], mas-CERT-UE, l-Europol u maċ-Ċentru ta' Analiżi tal-Intelligence tal-UE (INTCEN), se tikkontribwixxi wkoll għall-għarfien tas-sitwazzjoni fil-livell tal-UE. Dan jista' jiġi alimentat fl-intelligence dwar it-theddid u fit-tfassil tal-politika fil-kuntest ta' monitoraġġ regolari tax-xenarju tat-theddida u kooperazzjoni operazzjonali effettiva, kif ukoll b'rispons għal inċidenti transfruntiera fuq skala kbira.

[15] COM(2017) 477 final.

[16] 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.

[17] Kif previst fl-Artikolu 9 tad-Direttiva dwar iċ-Ċibersigurtà (NIS).

2.2 Lejn Att dwar Suq Uniku ta' Ċibersigurtà

It-tkabbir tas-suq taċ-ċibersigurtà fl-UE — f'termini ta' prodotti, servizzi u proċessi — jinżamm lura f'għadd ta' modi. Aspett fundamentali huwa n-nuqqas ta' skemi ta' ċertifikazzjoni taċ-ċibersigurtà rikonoxxuti madwar l-UE biex jibnu standards ogħla ta' reżiljenza fi prodotti u sabiex tissaħħaħ il-fiduċja fis-suq madwar l-UE kollha. Għaldaqstant, il-Kummissjoni qiegħda tressaq proposta għat-twaqqif ta' **qafas għaċ-ċertifikazzjoni taċ-ċibersigurtà tal-UE**[18]. lI-Qafas jistabbilixxi l-proċedura għall-ħolqien ta' skemi ta' ċertifikazzjoni għas-sigurtà ċibernetika mal-UE kollha, li jkopru prodotti, servizzi u/jew sistemi, li jadattaw il-livell ta' assigurazzjoni għall-użu involut (kemm jekk ikunu ta' infrastrutturi kritiċi jew apparat tal-konsumatur).[19]. Dan se jġib benefiċċji ċari għan-negozji billi jevita l-ħtieġa li jgħaddi minn bosta proċessi ta' ċertifikazzjoni meta jkun hemm kummerċ bejn il-fruntieri, u hekk jillimita l-ispejjeż amministrattivi u finanzjarji. L-użu ta' skemi żviluppati skont dan il-Qafas se jgħin ukoll biex tinbena l-fiduċja tal-konsumaturi, b'ċertifikat ta' konformità li jinforma u jassigura lix-xerrejja u lill-utenti magħrufa dwar il-karatteristiċi tas-sigurtà tal-prodotti u s-servizzi li jixtru u jużaw. Dan jagħmel l-istandards għoljin għas-sigurtà ċibernetika sors ta' vantaġġ kompetittiv. Ir-riżultat jibni reżiljenza ikbar minħabba li prodotti u servizzi tal-ICT jiġu evalwati b'mod formali kontra sett stabbilit ta' standards taċ-ċibersigurtà, li jista' jkun żviluppat b'rabta usa' mill-qrib mal-ħidma li għaddejja dwar l-istandards tal-ICT[20].

L-Iskemi ta' Qafas ikunu volontarji u ma joħolqu ebda obbligu regolatorju immedjat fuq bejjiegħa jew fornituri ta' servizzi. L-iskemi ma jikkontradixxu ebda rekwiżit ġuridiku applikabbli, bħalma hija l-leġiżlazzjoni tal-UE dwar il-protezzjoni tad-dejta.

Ladarba jiġi stabbilit il-Qafas, il-Kummissjoni se tistieden lill-partijiet interessati rilevanti biex jiffokaw fuq tliet oqsma ta' prijorità:

- Sigurtà f'applikazzjonijiet kritiċi jew b'riskju għoli[21]: sistemi li niddependu fuqhom fl-attivitajiet tagħna ta' kuljum, mill-karozzi tagħna għall-makkinarju fil-fabbriki, sal-akbar sistemi bħall-ajruplani jew l-impjanti li jiġġeneraw l-enerġija sal-iżgħar sistemi bħal apparat mediku, qed isiru dejjem aktar diġitali u interkonnessi. Għalhekk, il-komponenti ewlenin tal-ICT fi prodotti u sistemi bħal dawn jkunu jeħtieġu valutazzjonijiet rigoruż tas-sigurtà.

- Iċ-ċibersigurtà fi prodotti diġitali użati ħafna, netwerks, sistemi u servizzi użati mis-settur privat u pubbliku biex jiddefendu kontra attakki u japplikaw l-obbligi regolatorji [22] - bħal kriptaġġ tal-posta elettronika, firewalls u Networks Privati Virtwali; huwa kruċjali li l-użu dejjem aktar mifrux ta' dawn l-għodod ma jwassalx għal sorsi ġodda ta' riskju jew għal vulnerabbiltajiet ġodda.

- L-użu ta' metodi ta' "sigurtà sa mill-ippjanar" f'apparat diġitali bi prezz baxx, interkonness, tal-konsum tal-massa, apparati li jiffurmaw l-Internet tal-Oġġetti: jistgħu

[18] COM(2017) 477.

[19] Livell ta' assigurazzjoni jindika l-grad ta' rigorożità tal-valutazzjoni tas-sigurtà u normalment ikun proporzjonat mal-livell ta' riskju assoċjat mal-oqsma jew funzjonijiet ta' din l-applikazzjoni (jiġifieri livell għoli ta' assigurazzjoni meħtieġ għal prodotti jew servizzi tal-ICT użati f'riskju għoli ta' applikazzjoni jew funzjonijiet).

[20] COM(2016) 176.

[21] L-eċċezzjoni tkun jekk iċ-ċertifikazzjoni obbligatorja jew volontarja tkun irregolata minn atti oħra tal-Unjoni.

[22] Pereżempju, id-Direttiva (UE) 2016/1148, ir-Regolament (UE) 2016/679, id-Direttiva (UE) 2015/2366 u atti legali oħra bħall-Kodiċi Ewropea tal-Komunikazzjonijiet Elettroniċi, jeħtieġu li l-organizzazzjonijiet jimplimentaw miżuri ta' sigurtà xierqa biex jiġu indirizzati r-riskji tas-sigurtà ċibernetika rilevanti.

jintużaw skemi taħt il-qafas biex jindikaw li l-prodotti jinbnew bl-użu ta' metodi ta' żvilupp sikurtal-ogħla livell, li jkunu għaddew minn testijiet xierqa ta' sigurtà, u li l-bejjiegħa impenjaw ruħhom li jaġġornaw is-softwer tagħhom f'każ ta' theddid jew vulnerabbiltajiet ġodda skoperti reċentement.

Dawn il-prijoritajiet għandhom jieħdu kont partikolari, tax-xenarju tat-theddida taċ-ċibersigurtà li qed tevolvi, kif ukoll tal-importanza ta' servizzi essenzjali bħal servizzi tat-trasport, l-enerġija, il-kura tas-saħħa, il-banek, l-infrastrutturi tas-swieq finanzjarji, ilma tax-xorb jew l-infrastruttura diġitali[23].

Filwaqt li l-ebda prodott, sistema jew servizz tal-ICT ma jista' jkun iggarantit li huwa sikur"100 %", hemm diversi difetti magħrufa u ddokumentati sew fid-disinn ta' prodotti tal-ICT li jistgħu jiġu sfruttati għal attakki. Approċċ ta' "sigurtà skont id-disinn" adottat minn produtturi ta' apparati konnessi, softwer u apparat tal-IT jiżgura li ċ-ċibersigurtà tkun indirizzata qabel ma jitqiegħdu prodotti ġodda fis-suq. Dan jista' jkun parti mill-prinċipju ta' "dover ta' kura", li għandu jiġi żviluppat flimkien mal-industrija, li jista' jnaqqas il-vulnerabbiltajiet tal-prodott/tas-softwer bl-applikazzjoni ta' firxa ta' metodi mid-disinn, l-ittestjar u l-verifika, inkluż verifika formali fejn ikun applikabbli, manutenzjoni fit-tul, u l-użu ta' tagħmir sikur tal-iżvilupp, kif ukoll l-iżvilupp ta' proċessi, aġġornamenti u patches biex jindirizzaw il-vulnerabbiltajiet mhux skoperti qabel u aġġornament u tiswija malajr[24]. Dan se jżid ukoll il-fiduċja tal-konsumaturi fi prodotti diġitali.

Barra minn hekk, ir-rwol importanti ta' riċerkaturi tas-sigurtà ta' parti terza biex jiskopru l-vulnerabbiltajiet fi prodotti u servizzi eżistenti għandu jiġi rikonoxxut u l-kundizzjonijiet li jippermettu żvelar tal-vulnerabbiltà[25] koordinata għandhom jinħolqu fl-Istati Membri, u jibnu fuq l-aħjar prattiki[26] u standards rilevanti [27].

Fl-istess ħin, **diversi setturi** qed jaffaċċjaw kwistjonijiet speċifiċi u għandhom jiġu inkoraġġuti biex jiżviluppaw l-approċċ tagħhom stess. B'dan il-mod, l-istrateġiji ġenerali taċ-ċibersigurtà jkunu kkumplimentati minn strateġiji ta' ċibersigurtà speċifiċi għas-settur f'oqsma bħas-servizzi finanzjarji[28], l-enerġija, it-trasport u s-saħħa[29].

Il-Kummissjoni diġà enfasizzat il-kwistjonijiet speċifiċi dwar ir-**responsabbiltà** mqajma minn teknoloġiji diġitali ġodda[30] u għaddejja ħidma biex tanalizza l-implikazzjonijiet; il-passi li jmiss se jitlestew sa Ġunju 2018. Iċ-ċibersigurtà tqajjem kwistjonijiet madwar l-attribuzzjoni ta' ħsara għan-negozji u għall-ktajjen tal-provvista u jekk ma jiġux indirizzati

[23] Is-setturi fi ħdan il-kamp ta' applikazzjoni tad-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.

[24] Cybersecurity in the European Digital Single Market [Iċ-ċibersigurtà fis-Suq Uniku Diġitali Ewropew], Grupp ta' Livell Għoli ta' Konsulenti Xjentifiċi, Marzu 2017

[25] L-iżvelar tal-vulnerabbiltà koordinata huwa forma ta' kooperazzjoni li tiffaċilita u tippermetti lir-riċerkaturi tas-sigurtà biex jirrappurtaw il-vulnerabbiltajiet lis-sid jew lill-bejjiegħ tas-sistema ta' informazzjoni, u jagħti l-opportunità lill-organizzazzjoni biex tiddijanjostika u tirrimedja l-vulnerabbiltà b'mod korrett u f'waqtu qabel ma l-informazzjoni dettaljata dwar il-vulnerabbiltà tkun żvelata lil partijiet terzi jew lill-pubbliku.

[26] Pereżempju l-Prattika Tajba dwar l-Iżvelar tal-Vulnerabbiltà. Minn sfidi għal rakkomandazzjonijiet, ENISA, 2016

[27] ISO/IEC 29147: 2014 Teknoloġija tal-informatika — Tekniki ta' sikurezza — Vulnerabilità tal-iżvelar.

[28] Il-ħidma li jmiss tal-Kummissjoni dwar it-teknoloġija finanzjarja se tkopri ċ-ċibersigurtà għas-settur finanzjarju.

[29] Fis-settur tal-enerġija, pereżempju, il-kombinazzjoni ta' teknoloġiji tal-informazzjoni antiki ħafna u avvanzati ħafna, b'mod partikolari r-rekwiżiti f'ħin reali tal-grilja tal-enerġija.

[30] COM(2017) 228.

dawn il-kwistjonijiet jiġi mfixkel l-iżvilupp ta' suq uniku b'saħħtu fi prodotti u servizzi taċ-ċibersigurtà.

Fl-aħħar nett, l-iżvilupp tas-suq uniku tal-UE jiddependi wkoll fuq l-ikkunsidrar taċ-ċibersigurtà f'politika dwar il-kummerċ u l-investiment. L-effett ta' akkwisti barranin fuq it-teknoloġiji kritiċi - li ċ-ċibersigurtà hija eżempju importanti minnhom — hija aspett ewlieni fil-qafas għall-**iskrinjar ta' investiment dirett barrani fl-Unjoni Ewropea**[31], li għandu l-għan li jippermetti skrinjar ta' investimenti minn pajjiżi terzi għal raġunijiet ta' sigurtà u ta' ordni pubblika. Bl-istess mod, ir-rekwiżiti taċ-ċibersigurtà diġà ħolqu ostakoli lill-kummerċ għal prodotti u servizzi tal-UE f'setturi importanti f'numru ta' ekonomiji ta' pajjiżi terzi. Il-qafas għaċ-ċertifikazzjoni taċ-ċibersigurtà tal-UE se jkompli jsaħħaħ il-pożizzjoni internazzjonali tal-Ewropa, u għandu jiġi kkumplimentat minn sforzi kontinwi favur l-iżvilupp ta' standards globali ta' livell għoli ta' sigurtà u ftehimiet ta' rikonoxximent reċiproku.

2.3 L-Implimentazzjoni tad-Direttiva dwar is-Sigurtà tan-Netwerks u tas-Sistemi tal-Informazzjoni b'mod sħiħ

B'għodda prinċipali għall-ġlieda kontra ċ-ċibersigurtà llum f'idejn l-awtoritajiet nazzjonali, l-UE rrikonoxxiet il-ħtieġa li tgħolli l-istandards. L-inċidenti ta' ċibersigurtà fuq skala kbira rarament jaffettwaw biss Stat Membru wieħed, minħabba n-natura dejjem aktar globalizzata, dipendenti fuq id-diġitalità u n-natura interkonnessa ta' setturi ewlenin, bħal dak bankarju, tal-enerġija jew tat-trasport.

Id-Direttiva dwar is-Sigurtà tan-Netwerks u tas-Sistemi tal-Informazzjoni ("id-Direttiva NIS") hija l-ewwel liġi taċ-ċibersigurtà fl-UE kollha.[32]. Hija mfassla biex tibni r-reżiljenza billi ttejjeb il-kapaċitajiet taċ-ċibersigurtà nazzjonali; titrawwem kooperazzjoni aħjar bejn l-Istati Membri; u li tobbliga lill-impriżi f'setturi ekonomiċi importanti li jadottaw prattiki ta' ġestjoni effettiva tar-riskji u li jirrapportaw inċidenti serji lill-awtoritajiet nazzjonali. Dawn l-obbligi japplikaw ukoll għal tliet tipi ta' forniturі ta' servizzi tal-internet ewlenin: cloud computing, magni tat-tiftix u swieq onlajn. Din għandha l-għan li jkun hemm approċċ aktar sistematiku u fluss aħjar ta' informazzjoni.

L-implimentazzjoni sħiħa tad-Direttiva mill-Istati Membri kollha sa Mejju 2018 hija essenzjali għar-reżiljenza ċibernetika tal-UE. Dan il-proċess qed jiġi appoġġjat minn ħidma kollettiva mill-Istati Membri li sal-ħarifa tal-2017, se tirriżulta f'linji gwida biex tappoġġja implimentazzjoni aktar armonizzata, b'mod partikolari f'dak li għandu x'jaqsam ma' operaturi ta' servizzi essenzjali. Il-Kummissjoni qiegħda wkoll toħroġ Komunikazzjoni[33] bħala parti minn dan il-pakkett taċ-ċibersigurtà biex tappoġġja l-isforzi tagħhom billi tipprovdi l-aħjar prattiki mill-Istati Membri rilevanti għall-implimentazzjoni tad-Direttiva u gwida dwar il-mod li bih id-Direttiva għandha taħdem fil-prattika.

Żona fejn id-Direttiva ser ikollha tiġi supplimentata hija l-fluss ta' informazzjoni. Pereżempju, id-Direttiva tkopri biss setturi strateġiċi ewlenin — iżda loġikament metodu simili użat mill-partijiet interessati kollha milquta minn attakki ċibernetiċi huwa essenzjali biex ikun hemm valutazzjoni sistematika tal-vulnerabbiltajiet u punti ta' dħul tal-awturi għal attakki ċibernetiċi. Barra minn hekk, il-kooperazzjoni u l-qsim tal-informazzjoni bejn is-settur pubbliku u dak privat qed tiffaċċja għadd ta' ostakli. Gvernijiet u awtoritajiet pubbliċi

[31] COM(2017) 478.

[32] 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.

[33] COM(2017) 476.

mhumiex disposti li jaqsmu informazzjoni rilevanti għaċ-ċibersigurtà minħabba l-biża' li tikkompromett s-sigurtà nazzjonali jew il-kompetittività. Impriżi privati jsibuha bi tqila biex jaqsmu informazzjoni dwar il-vulnerabbiltajiet ċibernetiċi u telf li kien ikkawżat minħabba l-biża' li tikkompromett informazzjoni kummerċjali sensittiva, u dan iġib miegħu riskju għar-reputazzjoni tagħhom, jew jirriskjaw li jiksru r-regoli dwar il-protezzjoni tad-dejta[34]. Jeħtieġ li tissaħħaħ il-fiduċja għal sħubijiet pubbliċi-privati biex tiġi sostnuta kooperazzjoni usa' u l-kondiviżjoni tal-informazzjoni fost numru ikbar ta' setturi. Ir-rwol taċ-Ċentri ta' Kondiviżjoni ta' Informazzjoni u ta' Analiżi huwa partikolarment importanti fil-ħolqien tal-fiduċja meħtieġa għall-kondiviżjoni tal-informazzjoni bejn is-settur privat u dak pubbliku. L-ewwel passi ttieħdu f'ċerti setturi kritiċi bħalma huma l-avjazzjoni, permezz tal-ħolqien taċ-Ċentru Ewropew għaċ-Ċibersigurtà fl-Avjazzjoni[35], u l-enerġija, permezz tal-iżvilupp ta' Ċentri ta' Kondiviżjoni ta' Informazzjoni u ta' Analiżi[36]. Il-Kummissjoni se tikkontribwixxi b'mod sħiħ għal dan l-approċċ, bl-appoġġ tal-ENISA, u huwa meħtieġ aċċellerar b'mod partikolari f'dak li għandu x'jaqsam ma' setturi li jipprovdu servizzi essenzjali kif identifikati mid-Direttiva dwar iċ-Ċibersigurtà (NIS).

2.4 Reżiljenza permezz ta' rispons rapidu ta' emerġenza

Meta jseħħ attakk ċibernetiku, rispons malajr u effettiv jista' jtaffi l-impatt tiegħu. Dan jista' wkoll juri li l-awtoritajiet pubbliċi ma jkunux mingħajr saħħa meta jiġu ffaċċjati minn attakki ċibernetiċi, u jikkontribwixxu biex tinbena l-fiduċja. F'dak li għandu x'jaqsam mar-rispons tal-istituzzjonijiet tal-UE stess, fl-ewwel istanza l-aspetti ċibernetiċi għandhom ikunu integrati fil-mekkaniżmi eżistenti tal-UE għall-ġestjoni ta' kriżijiet: ir-rispons integrat tal-kriżi politika tal-UE, koordinat mill-Presidenza tal-Kunsill[37] u s-sistemi ta' twissija bikrija tal-UE[38]. Il-ħtieġa ta' rispons għal inċident jew attakk ċibernetiku partikolarment sejru tista' tkun biżżejjed biex Stat Membru jinvoka l-Klawżola ta' Solidarjetà tal-UE.[39].

Rispons malajr u effettiv jiddependi wkoll fuq mekkaniżmu ta' skambju rapidu ta' informazzjoni bejn l-atturi ewlenin kollha fil-livell nazzjonali u tal-UE, li min-naħa tagħhom jeħtieġu ċarezza dwar ir-rwoli u r-responsabbiltajiet rispettivi tagħhom. Il-Kummissjoni kkonsultat lill-istituzzjonijiet u l-Istati Membri tagħha dwar "Pjan ta' Azzjoni" biex tipprovdi proċess effettiv għal rispons operazzjonali fil-livell tal-Unjoni u tal-Istati Membri, għal inċident ċibernetiku mifrux. Il-**Pjan ta' Azzjoni**ppreżenta f'Rakkomandazzjoni[40] f'dan il-pakkett jispjega kif iċ-ċibersigurtà tiġi integrata fil mekkaniżmi ta' Maniġġjar ta' Kriżijiet eżistenti fil-livell tal-UE u jistabbilixxi l-objettivi u l-modalitajiet ta' kooperazzjoni bejn l-Istati Membri, kif ukoll bejn l-Istati Membri u l-istituzzjonijiet rilevanti tal-UE, is-servizzi, l-

---

[34] Cybersecurity in the European Digital Single Market [Iċ-ċibersigurtà fis-Suq Uniku Diġitali Ewropew], grupp ta' Livell Għoli ta' Konsulenti Xjentifiċi, Marzu 2017. Kwistjoni partikolari tikkonċerna s-sigrieti kummerċjali, fejn il-Komunikazzjoni ta' Lulju 2016 "Insaħħu r-Reżiljenza tal-UE għaċ-Ċibersigurtà" innutat ir-reżistenza biex jiġi rappurtat is-serq ta' sigrieti kummerċjali u l-importanza ta' mezzi affidabbli għar-rappurtar li jiżguraw il-kunfidenzjalità.

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

[36] Dawn huma organizzazzjonijiet mingħajr skop ta' qligħ, immexxija mill-membri ffurmati minn entitajiet privati u pubbliċi biex jaqsmu informazzjoni dwar it-theddid ċibernetiku, ir-riskji, il-prevenzjoni, il-mitigazzjoni u r-rispons. Ara eż. iċ-Ċentri ta' Kondiviżjoni ta' Informazzjoni u ta' Analiżi tal-Enerġija Ewropea (http://www.ee-isac.eu).

[37] Dan jippermetti għall-koordinazzjoni tar-rispons għall-kriżijiet il-kbar transettorjali fl-ogħla livell politiku.

[38] Dawn jippermettu l-kondiviżjoni u l-koordinazzjoni ta' informazzjoni interna dwar kriżijiet multisettorali emerġenti jew theddid prevedibbli jew imminenti li jeħtieġ azzjoni fuq il-livell tal-UE.

[39] Skont l-Artikolu 222 tat-Trattat dwar il-Funzjonament tal-Unjoni Ewropea.

[40] C(2017) 6100.

aġenziji u l-korpi[41] tal-UE fir-rispons tagħhom għal inċidenti u kriżijiet ta' ċibersigurtà fuq skala kbira. Ir-Rakkomandazzjoni titlob ukoll lill-Istati Membri u lill-istituzzjonijiet tal-UE biex jistabbilixxu Qafas ta' Rispons għall-Kriżi taċ-Ċibersigurtà tal-UE biex jitħaddem il-pjan. Il-pjan ta' Azzjoni se jiġi ttestjat regolarment b'eżerċizzji ta' ġestjoni tal-kriżijiet ċibernetiċi u oħrajn[42] u se jiġi aġġornat kif meħtieġ.

Minħabba li l-inċidenti ta' ċibersigurtà jista' jkollhom impatt sostanzjali fuq il-funzjonament tal-ekonomiji u fuq il-ħajja ta' kuljum tan-nies, waħda mill-għażliet tista' tkun li tiġi investigata l-possibbiltà ta' **Fond għar-Rispons ta' Emerġenza taċ-Ċibersigurtà**, fuq l-eżempju ta' mekkaniżmi ta' kriżi oħra ta' dan it-tip f'oqsma ta' politika oħrajn tal-UE. Dan jippermetti lill-Istati Membri biex ifittxu l-għajnuna fil-livell tal-UE matul jew wara inċident kbir, dment li l-Istat Membru jkun implementa sistema prudenti ta' ċibersigurtà qabel l-inċident, inkluża l-implimentazzjoni sħiħa tad-Direttiva NIS, ġestjoni tar-riskju matura u oqfsa superviżorji fil-livell nazzjonali. Fond bħal dan, li jikkumplimenta l-mekkaniżmi eżistenti għall-ġestjoni tal-kriżijiet fil-livell tal-UE, jista' juża l-kapaċità ta' tweġiba rapida fl-interessi tas-solidarjetà u jiffinanzja azzjonijiet ta' rispons għall-emerġenzi speċifiċi bħas-sostituzzjoni ta' apparat kompromess jew l-użu ta' għodod ta' mitigazzjoni jew ta' rispons, billi jibbaża ruħu fuq l-għarfien espert nazzjonali skont il-Mekkaniżmu tal-UE għall-Protezzjoni Ċivili.

2.5 Netwerk ta' kompetenza ta' ċibersigurtà b'Ċentru Ewropew ta' Riċerka u Kompetenza taċ-Ċibersigurtà

L-għodda teknoloġiċi ta' ċibersigurtà huma assi strateġiċi, kif ukoll teknoloġiji ewlenin ta' tkabbir għall-futur. Huwa fl-interess strateġiku tal-UE li tiżgura li l-UE żżomm u tiżviluppa l-kapaċitajiet essenzjali biex tiżgura l-ekonomija diġitali, is-soċjetà u d-demokrazija tagħha, biex tipproteġi l-ħardwer u s-softwer kritiċi u biex tipprovdi servizzi ta' ċibersigurtà ewlenin.

L-Isħubija Pubblika-Privata dwar iċ-Ċibersigurtà[43] maħluqa fl-2016 kienet l-ewwel pass importanti, li skattat investiment sa massimu ta' EUR 1.8 biljun sal-2020. Madankollu, l-iskala tal-investiment f'partijiet oħra tad-dinja[44] tissuġġerixxi li l-UE għandha bżonn tagħmel aktar f'termini ta' investiment biex tegħleb il-frammentazzjoni tal-kapaċitajiet mifruxa madwar l-UE.

L-UE għandha valur miżjud minħabba li s-sofistikazzjoni tat-teknoloġija taċ-ċibersigurtà tipprovdi l-investiment meħtieġ fuq skala kbira u l-ħtieġa għal soluzzjonijiet li jaħdmu f'pajjiżi oħra tal-UE. Filwaqt li tibni fuq il-ħidma tal-Istati Membri u tas-Sħubija Pubblika-Privata, pass ulterjuri jkun li tiġi rinfurzata l-kapaċità taċ-ċibersigurtà tal-UE permezz ta' **netwerk ta' ċentri ta' kompetenza taċ-ċibersigurtà**[45] b'**Ċentru Ewropew ta' Riċerka u Kompetenza taċ-Ċibersigurtà**fil-qalba tagħha. Dan in-netwerk u ċ-Ċentru tiegħu jistimulaw l-iżvilupp u l-użu tat-teknoloġija fiċ-ċibersigurtà u jikkomplementaw l-isforzi tal-bini tal-kapaċità f'dan il-qasam fuq livell tal-UE u fuq dak nazzjonali. Il-Kummissjoni ser tniedi

---

[41] Inkluż l-Europol, l-ENISA, l-Iskwadra ta' Rispons f'Emerġenza relatata mal-Kompjuters tal-UE għall-istituzzjonijiet, il-korpi u l-aġenziji tal-UE (CERT-EU) u ċ-Ċentru ta' Analiżi tal-Intelligence tal-UE (INTCEN).

[42] Pereżempju, dawk immexxija mill-ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

[43] C(2016) 4400 final.

[44] Fl-2017 biss, l-Istati Uniti se tinvesti 19-il biljun dollaru fiċ-ċibersigurtà, żieda ta' 35 % meta mqabbla mal-2016. Il-White House, l-Uffiċċju tas-Segretarju tal-Istampa: 'Skeda Informattiva: "Il-Pjan ta' Azzjoni Nazzjonali dwar iċ-Ċibersigurtà"', id-9 ta' Frar 2016.

[45] In-netwerk jista' jinkludi ċentri eżistenti u futuri fiċ-ċiberasigurtà mwaqqfa fl-Istati Membri, li l-membri tagħhom ikunu tipikament organizzazzjonijiet pubbliċi tar-riċerka u laboratorji.

valutazzjoni tal-impatt li teżamina l-alternattivi disponibbli — inkluż il-possibbiltà li tiġi stabbilita Impriża Konġunta — bl-għan li titwaqqaf din l-istruttura fl-2018.

Bħala l-ewwel pass u sabiex tinforma l-ħsieb fil-futur, il-Kummissjoni se tipproponi li titnieda fażi pilota taħt Orizzont 2020, biex iċ-ċentri nazzjonali jinġiebu flimkien f'netwerk biex jinħoloq momentum ġdid fil-kompetenza taċ-ċibersigurtà u l-iżvilupp tat-teknoloġija. Għalhekk il-Kummissjoni qed tippjana li tipproponi injezzjoni ta' fondi fuq żmien qasir ta' EUR 50 miljun. Din l-attività se tikkumplimenta l-implimentazzjoni li għaddejja bħalissa tas-Sħubija Pubblika-Privata dwar iċ-Ċibersigurtà.

L-isforzi ta' riċerka tal-għaqda u l-formazzjoni se jkunu fil-qalba tan-netwerk u l-enfasi inizjali taċ-Ċentru. Biex tappoġġja l-iżvilupp ta' kapaċitajiet industrijali, iċ-Ċentru jista' jaġixxi bħala maniġer tal-proġett ta' kapaċità li jista' jimmaniġġja proġetti multinazzjonali. Dan jista' wkoll jagħti spinta żejda lill-innovazzjoni u l-kompetittività tal-industrija tal-UE fix-xena globali fl-iżvilupp ta' teknoloġiji diġitali tal-ġenerazzjoni li jmiss inkluża l-intelliġenza artifiċjali, il-quantum computing, blockchain u identitajiet diġitali siguri, kif ukoll fl-iżgurar tal-aċċess għad-dejta tal-massa għall-kumpaniji bbażati fl-UE, li kollha huma ewlenin għaċ-ċibersigurtà fil-futur. Iċ-Ċentru se jibni wkoll fuq il-ħidma tal-UE biex jiżviluppa l-infrastruttura dwar l-Informatika ta' Prestazzjoni Għolja: dan huwa essenzjali għall-analiżi ta' kwantitajiet kbar ta' dejta, il-kriptaġġ u d-dekriptaġġ tad-dejta, il-verifika ta' identitajiet, is-simulazzjoni ta' attakki ċibernetiċi, u l-analiżi ta' materjal viżiv[46].

In-netwerk ta' ċentri ta' kompetenza jista' jkollu wkoll il-kapaċitajiet biex jappoġġja l-industrija permezz ta' testijiet u ta' simulazzjoni biex jirfed iċ-ċertifikazzjoni ta-ċibersigurtà deskritta fit-taqsima 2.2. L-involviment tiegħu fil-firxa sħiħa ta' attività taċ-ċibersigurtà tal-UE jiggarantixxi aġġornament kontinwu tal-istrateġiji tiegħu skont il-ħtieġa. Iċ-Ċentru se jimmira biex jixpruna standards għoljin ta' ċibersigurtà mhux biss f'sistemi tat-teknoloġija u ta' ċibersigurtà iżda wkoll fl-iżvilupp ta' ħiliet ta' livell għoli għal professjonisti, billi jipprovdi soluzzjonijiet u mudelli għall-isforzi nazzjonali biex jiġu introdotti l-ħiliet diġitali. F'dan ir-rigward, għandu jtejjeb ukoll il-kapaċitajiet taċ-ċibersigurtà fil-livell tal-UE u jibni fuq sinerġiji b'mod partikolari mal-ENISA, is-CERT-EU, l-Europol, il-Fond għar-Rispons ta' Emerġenza taċ-Ċibersigurtà possibbli tal-futur u s-CSIRTs nazzjonali.

Fokus partikolari ta' ħidma permezz tan-netwerk ta' kompetenza għandu jkun in-nuqqas ta' kapaċità Ewropea dwar il-**kriptaġġ** ta' prodotti u servizzi użati miċ-ċittadini, negozji u gvernijiet fi ħdan is-Suq Uniku Diġitali. Kriptaġġ qawwi huwa l-bażi għal sistemi ta' identifikazzjoni diġitali sigura li taqdi rwol ewlieni fiċ-ċibersigurtà effettiva[47]; barra minn hekk din iżżomm il-proprjetà intellettwali tan-nies sigura u tippermetti l-protezzjoni tad-drittijiet fundamentali bħalma huma l-libertà tal-espressjoni u l-protezzjoni tad-dejta personali, u tiżgura kummerċ sikur onlajn[48].

Hekk kif is-swieq taċ-ċibersigurtà ċivili u tad-difiża tal-UE jikkondividu sfidi komuni[49] u t-teknoloġija b'użu doppju li jeħtieġu kollaborazzjoni mill-qrib f'oqsma kritiċi, tista' tiġi żviluppata t-tieni fażi tan-netwerk u taċ-Ċentru tagħha b'dimensjoni tad-difiża ċibernetika, b'rispett sħiħ tad-dispożizzjonijiet tat-Trattat relatati mal-Politika ta' Sigurtà u ta' Difiża Komuni. Minbarra l-iffukar fuq it-teknoloġika tagħha, id-dimensjoni tad-difiża tista'

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

[47] Il-Kummissjoni diġà se tniedi sfida ġdida għall-Premju Orizzont taħt Orizzont 2020 li ser tagħti EUR 4 miljuni għall-aħjar soluzzjoni innovattiva għal metodi ta' awtentikazzjoni online bla xkiel.

[48] Cybersecurity in the European Digital Single Market [Iċ-ċibersigurtà fis-Suq Uniku Diġitali Ewropew], grupp ta' Livell Għoli ta' Konsulenti Xjentifiċi, Marzu 2017.

[49] "Studju dwar sinerġiji bejn is-swieq taċ-ċibersigurtà ċivili u tad-difiża" (Optimity; SMART 2014-0059).

tikkontribwixxi għall-kooperazzjoni bejn l-Istati Membri fil-qasam taċ-ċiberdifiża, inkluż il-kondiviżjoni ta' informazzjoni, l-għarfien tas-sitwazzjoni, il-bini ta' għarfien espert u r-rispons koordinat, u tista' tappoġġja l-iżvilupp tal-Istati Membri ta' kapaċitajiet komuni. Din tista' wkoll taġixxi bħala pjattaforma, li tippermetti lill-Istati Membri jidentifikaw il-prijoritajiet għad-difiża ċibernetika tal-UE, tinvestiga soluzzjonijiet komuni, tikkontribwixxi għall-iżvilupp ta' strateġiji komuni, tiffaċilita t-taħriġ tad-difiża ċibernetika konġunt, l-eżerċitar u l-ittestjar fil-livell Ewropew, u tappoġġja x-xogħol dwar tassonomiji u standards tad-difiża ċibernetika, bir-rwol taċ-Ċentru jkun wieħed ta' appoġġ u konsultattiv. Biex iwettaq l-attivitajiet imsemmija hawn fuq, iċ-Ċentru jkollu bżonn jaħdem fil-qrib u b'komplementarjetà sħiħa mal-Aġenzija Ewropea għad-Difiża fil-qasam taċ-ċiberdifiża, kif ukoll mal-ENISA fil-qasam tar-reżiljenza ċibernetika. Din id-dimensjoni tad-difiża tqis il-proċess imniedi mill-Karta ta' riflessjoni dwar il-futur tad-Difiża Ewropea.

Il-livell għoli ta' reżiljenza meħtieġa fil-qasam tad-difiża ċibernetika jitlob miri speċifiċi ta' sforzi ta' riċerka u teknoloġija. Il-proġetti ta' difiża ċibernetika jew tat-teknoloġiji żviluppati minn impriżi jistgħu jibbenefikaw minn finanzjament tal-Fond Ewropew għad-Difiża meta jiġu kemm għall-fażi tar-riċerka kif ukoll tal-iżvilupp[50]. Oqsma speċifiċi bħalma huma sistemi ta' kriptaġġ ibbażati fuq teknoloġiji quantum, l-għarfien tas-sitwazzjoni taċ-ċibersigurtà, is-sistemi ta' kontroll tal-aċċess bijometriku, id-detezzjoni ta' Theddid Persistenti Avvanzat, jew l-estrazzjoni ta' dejta jistgħu jkunu partikolarment rilevanti f'dan il-kuntest. Ir-Rappreżentant Għoli, l-Aġenzija Ewropea għad-Difiża u l-Kummissjoni se jappoġġjaw lill-Istati Membri fl-identifikazzjoni ta' oqsma fejn il-proġetti komuni taċ-ċibersigurtà jistgħu jitqiesu għal finanzjament mill-Fond Ewropew għad-Difiża.

2.6 Il-bini ta' bażi ta' ħiliet ċibernetiċi b'saħħitha tal-UE

Hemm dimensjoni edukattiva qawwija għaċ-ċibersigurtà. Iċ-ċibersigurtà effettiva tiddependi ħafna fuq il-ħiliet tal-persuni kkonċernati. Iżda d-distakk tal-ħiliet taċ-ċibersigurtà għall-professjonisti li jaħdmu fis-settur privat fl-Ewropa huwa mbassar li jiżdied għal 350,000 sal-2022[51]. Għandha tiġi żviluppata edukazzjoni dwar iċ-ċibersigurtà fil-livelli kollha, ibda minn taħriġ regolari ta' forza tax-xogħol ċibernetika, taħriġ addizzjonali fiċ-ċibersigurtà għall-ispeċjalisti kollha tal-ICT, u kurrikula speċifiċi ta' ċibersigurtà ġodda. Għandhom jiġu stabbiliti ċentri ta' kompetenza akkademika b'saħħithom biex ilaħħqu mad-domanda għal edukazzjoni u taħriġ aċċellerat, li għandhom jimxu fuq il-gwida minn Ċentru Ewropew għar-Riċerka u l-Kompetenza taċ-Ċibersigurtà u l-ENISA. L-għan għandu jkun li ssir naturali biex jiġu mfassla prodotti u sistemi tal-ICT li jinkorporaw il-prinċipji ta' sigurtà sa mill-bidu nett. L-edukazzjoni taċ-ċibersigurtà m'għandhiex tkun limitata biss għal professjonisti fil-qasam tal-IT, iżda għandha tiġi integrata fil-kurrikuli ta' oqsma oħrajn, bħalma huma l-inġinerija, il-ġestjoni tan-negozju jew tad-dritt, kif ukoll għall-binarji ta' edukazzjoni speċifiċi għas-settur. Fl-aħħar nett, l-għalliema u l-istudenti fl-edukazzjoni primarja u sekondarja għandhom jiġu sensibilizzati dwar iċ-ċiberkriminalità u ċ-ċibersigurtà meta jakkwistaw kompetenzi diġitali fl-iskejjel.

[50] Il-Programm tal-Iżvilupp tal-Industrija tad-Difiża Ewropea diġà ser jagħti prijorità lil proġetti ta' ċiberdifiża u ċ-ċiberdifiża se tkun waħda mit-temi tas-sejħa għall-proposti li se jiġu mnedija fl-2018.

[51] Stħarriġ tal-2017 dwar il-Forza tax-Xogħol fis-Settur tas-Sigurtà tal-Informazzjoni Globali. In-nuqqas globali huwa ta' 1.8 miljun.

L-UE, flimkien mal-Istati Membri, għandha wkoll tagħti kontribut għal din il-ħidma billi tibni fuq il-ħidma tal-Koalizzjoni għall-Ħiliet u l-Impjiegi Diġitali[52] u billi pereżempju ddaħħal fis-seħħ, skemi ta' apprendistat fiċ-ċibersigurtà għall-SMEs.

2.7 Il-promozzjoni ta' iġjene ċibernetika u sensibilizzazzjoni

B'madwar 95 % tal-inċidenti li huma possibbli permezz ta' "xi tip ta' żball uman — intenzjonat jew le",[53] xorta hemm fattur uman involut. B'hekk iċ-ċibersigurtà hija r-responsabbiltà ta' kulħadd. Dan ifisser li hemm bżonn bidla fl-imġiba personali, korporattiva u fl-amministrazzjoni pubblika biex jiġi żgurat li kulħadd jifhem it-theddida, u jkun mgħammar bl-għodod u l-ħiliet meħtieġa biex jipproteġi lilu nnifsu malajr u b'mod attiv kontra l-attakki. Hemm bżonn li n-nies jiżviluppaw drawwiet ta' iġjene ċibernetika u n-negozji u l-organizzazzjonijiet għandhom jadottaw programmi xierqa bbażati fuq ir-riskji taċ-ċibersigurtà u jaġġornawhom b'mod regolari biex jirriflettu x-xenarju tar-riskju li qed jevolvi.

Id-Direttiva dwar iċ-Ċibersigurtà (NIS) mhux biss tistabbilixxi r-responsabbiltajiet tal-Istati Membri biex jiskambjaw informazzjoni dwar attakki ċibernetiċi fil-livell tal-UE, iżda wkoll tqiegħed fis-seħħ strateġiji maturi taċ-ċibersigurtà u oqfsa nazzjonali għas-sigurtà tan-netwerks u tas-sistemi tal-informazzjoni. Amministrazzjonijiet pubbliċi fil-livell tal-UE u nazzjonali għandu jkollhom rwol aktar ewlieni fl-ixprunar ta' dawn l-isforzi.

L-ewwel nett, l-Istati Membri għandhom jimmassimizzaw id-disponibbiltà ta' għodod taċ-ċibersigurtà għal negozji u individwi. B'mod partikolari, hemm bżonn li jsir aktar għall-prevenzjoni u l-mitigazzjoni tal-impatti taċ-ċiberkriminalità fuq l-utenti finali. Diġà jeżisti eżempju fil-ħidma tal-Europol mal-kampanja "NoMoreRansom"[54], żviluppata permezz ta' kooperazzjoni mill-qrib bejn l-eżekuzzjoni tal-liġi u l-kumpaniji taċ-ċibersigurtà biex jgħinu lill-utenti jipprevjenu infezzjonijiet ransomware u jiddeċifraw id-dejta jekk ikunu vittmi ta' attakk. Skemi bħal dawn għandhom ikunu introdotti għal tipi oħrajn ta' malwer, f'oqsma oħra u l-UE għandha tiżviluppa **portal uniku li jiġbor flimkien dawn l-għodod kollha f'punt uniku ta' servizz (one-stop-shop)**, li joffri pariri lill-utenti dwar il-prevenzjoni u l-iskoperta ta' malwer u rabtiet ma' mekkaniżmi ta' rappurtar.

It-tieni nett, l-Istati Membri għandhom iħaffu l-**użu ta' aktar għodod ċibersiguri fl-iżvilupp tal-gvern elettroniku** u wkoll jiġbru l-benefiċċji kollha minn fuq in-netwerk ta' kompetenza. L-adozzjoni ta' mezzi sikuri ta' identifikazzjoni għandhom jiġu promossi, filwaqt li tibni fuq il-qafas tal-UE ta' identifikazzjoni elettronika u servizzi fiduċjarji għal tranżazzjonijiet elettroniċi fis-suq intern, li ilhom fis-seħħ mill-2016 u jipprovdu ambjent regolatorju prevedibbli li jippermetti l-interazzjonijiet elettroniċi sikuri u bla intoppi bejn negozji, individwi u awtoritajiet pubbliċi[55]. Barra minn hekk, istituzzjonijiet pubbliċi, speċjalment dawk li jipprovdu servizzi essenzjali, għandhom jiżguraw li l-persunal tagħhom huwa mħarreġ f'oqsma relatati maċ-ċibersigurtà.

It-tielet nett, l-Istati Membri għandhom jagħmlu s-sensibilizzazzjoni ċiber bħala prijorità f'**kampanji ta' sensibilizzazzjoni**, inklużi dawk immirati lejn l-iskejjel, l-universitajiet, il-

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] L-"Indiċi ta' Intelliġenza taċ-Ċibersigurtà" IBM tal-2014, imsemmija f'Securitymagazine.com, 19 ta' Ġunju 2014.

[54] https://www.nomoreransom.org/.

[55] Ir-Regolament (UE) 910/2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal transazzjonijiet elettroniċi fis-suq intern (ir-Regolament eIDAS) adottat fit-23 ta' Lulju 2014. Barra minn hekk, il-Kummissjoni Ewropea qed tipprovdi elementi importanti u għodod għall-identifikazzjoni elettronika u l-interoperabbiltà tal-Firma elettronika (eż. Listi ta' Fiduċja ta' Brawżers) permezz tal-Programm tal-Faċilità Nikkollegaw l-Ewropa.

komunità tan-negozju u l-korpi ta' riċerka. Ix-xahar għas-Sigurtà Ċibernetika li jsir kull sena f'Ottubru, taħt il-koordinazzjoni tal-ENISA, se jitwessa' biex jintlaħqu aktar nies fl-isforz ta' komunikazzjoni komuni fil-livell tal-UE u f'dak nazzjonali. It-tqajjim ta' sensibilizzazzjoni f'dak li għandu x'jaqsam ma' **kampanji online ta' diżinformazzjoni u aħbarijiet foloz** fuq il-midja soċjali mmirati speċifikament li jimminaw il-proċessi demokratiċi u l-valuri Ewropej huwa ugwalment importanti. Filwaqt li r-responsabbiltà primarja tibqa' fil-livell nazzjonali — inkluż għall-elezzjonijiet tal-Parlament Ewropew — il-ġbir ta' għarfien u l-qsim ta' esperjenzi fil-livell Ewropew wera li huwa ta' valur miżjud billi jipprovdu fokus għal azzjoni[56].

Hemm ukoll rwol bsaħħtu għall-**industrija** b'mod ġenerali, iżda b'attenzjoni partikolari għal forniturі ta' servizzi diġitali u manifatturi. Jeħtieġ li jappoġġja l-utenti (individwi, negozji u amministrazzjonijiet pubbliċi) b'għodod li jippermettulhom jieħdu r-responsabbiltà għall-azzjonijiet tagħhom online, billi jagħmilha ċara li ż-żamma taċ-ċiberiġjene hija parti indispensabbli mill-offerta lill-konsumaturi[57]. Biex issib u tneħħi vulnerabbiltajiet, l-industrija għandha taħdem sabiex ikollha proċessi interni li jittrattaw l-investigazzjoni, tikklassifika u ssolvi vulnerabbiltajiet, indipendentement minn jekk is-sors ta' vulnerabbiltà potenzjali kienx estern jew fi ħdan il-kumpanija kkonċernata.

Azzjonijiet ewlenin

- L-implimentazzjoni sħiħa tad-Direttiva dwar is-Sigurtà tan-Netwerks u tas-Sistemi tal-Informazzjoni;
- L-adozzjoni rapida mill-Parlament Ewropew u mill-Kunsill tar-Regolament li jistabbilixxi mandat ġdid għal ENISA u qafas Ewropew għaċ-ċertifikazzjoni[58];
- Inizjattiva konġunta tal-Kummissjoni/tal-industrija għad-definizzjoni tal-prinċipju "dover ta' kura" għat-tnaqqis tal-vulnerabbiltajiet tal-prodott/tas-softwer u l-promozzjoni ta' "sigurtà permezz tad-disinn";
- Implimentazzjoni rapida ta' pjan ta' azzjoni f'każ ta' inċident ewlieni transfruntier;
- It-tnedija ta' valutazzjoni tal-impatt biex tistudja l-possibbiltà għal proposta tal-Kummissjoni fl-2018 biex jiġi stabbilit Netwerk ta' Ċentri ta' kompetenza dwar iċ-ċibersigurtà u Ċentru għaċ-Ċibersigurtà Ewropea u Ċentru ta' Kompetenza, li tibni fuq il-fażi pilota immedjata;
- Appoġġ lill-Istati Membri fl-identifikazzjoni ta' oqsma fejn jistgħu jiġu kkunsidrati proġetti taċ-ċibersigurtà komuni għall-appoġġ mill-Fond Ewropew għad-Difiża;
- Punt uniku ta' servizz għall-UE kollha biex jgħin lill-vittmi ta' attakki ċibernetiċi, u għoti ta' informazzjoni dwar l-aħħar theddid u l-ġbir flimkien tal-aħħar pariri prattiċi u tal-għodod taċ-ċibersigurtà;
- Azzjoni mill-Istati Membri biex tintegra ċ-ċibersigurtà fi programmi ta' ħiliet, il-gvern elettroniku u kampanji ta' sensibilizzazzjoni;
- Azzjoni min-naħa tal-industrija biex jiżdied it-taħriġ relatat maċ-ċibersigurtà għall-persunal tagħhom u jadottaw approċċ ta' "sigurtà permezz tad-disinn" għall-prodotti, is-

[56] Eżempju ta' dan huwa t-Task Force East StratCom stabbilit fl-2015 mill-Istati Membri u mir-Rappreżentant Għoli sabiex jindirizza rispons għall-kampanji Russi ta' diżinformazzjoni li attwalment għaddejjin. L-iskwadra hi involuta f'prodotti ta' żvilupp ta' komunikazzjoni u kampanji iffukati li jispjegaw il-politiki tal-UE fir-reġjun tas-Sħubija tal-Lvant.

[57] Xi manifatturi diġà draw dan il-kunċett kif ukoll mil-leġiżlazzjoni Ewropea dwar il-prodotti (bħad-Direttiva dwar il-Makkinarju 2006/42/KE) jistipula l-prinċipji għal "sigurtà permezz tad-disinn".

[58] COM(2017) 477.

servizzi u l-proċessi tagħhom.

3. IL-ĦOLQIEN TA' DETERRENZA ĊIBERNETIKA EFFETTIVA TAL-UE

Deterrenza effettiva tfisser tqiegħed fis-seħħ qafas ta' miżuri li huma kemm kredibbli kif ukoll konvinċenti għal dawk li jixtiequ jkunu kriminali u aggresuri ċibernetiċi. Sakemm l-awturi ta' attakki ċibernetiċi — kemm statali u mhux statali — m'għandhomx minn xiex jibżgħu minbarra l-falliment, huma mhux se jkollhom inċentiv kbir biex ikomplu jippruvaw. Rispons ta' infurzar tal-liġi aktar effettiv li jiffoka fuq l-identifikazzjoni, l-intraċċar u l-prosekuzzjoni tal-kriminali ċibernetiċi huwa ċentrali għall-bini ta' deterrenza effettiva. Flimkien ma' dan hija l-ħtieġa li l-UE tappoġġja l-Istati Membri fl-iżvilupp ta' kapaċitajiet b'użu doppju taċ-ċibersigurtà. Inkunu nistgħu naqilbu għal xejra ġdida dwar l-attakki ċibernetiċi meta nżidu l-possibbiltajiet li wieħed jinqabad u jiġi sanzjonat għat-twettiq tagħhom. L-attakki ċibernetiċi għandhom jiġu investigati fil-pront u l-awturi responsabbli għandhom jitressqu quddiem il-ġustizzja, jew tittieħed azzjoni sabiex ikun hemm rispons politiku jew diplomatiku xieraq. F'każ ta' kriżi ewlenija b'dimensjoni internazzjonali importanti u ta' difiża, ir-Rappreżentanta Għolja tista' tippreżenta opzjonijiet għal rispons xieraq lill-Kunsill.

Pass wieħed lejn it-titjib tar-rispons tal-liġi kriminali għal attakki ċibernetiċi diġà ttieħed bl-adozzjoni fl-2013 tad-Direttiva dwar attakki kontra s-sistemi tal-informazzjoni[59]. Dan jistabbilixxi regoli minimi li jikkonċernaw id-definizzjoni ta' reati kriminali u sanzjonijiet fil-qasam tal-attakki kontra s-sistemi tal-informazzjoni u pprovda għal miżuri operazzjonali biex titjieb il-kooperazzjoni fost l-awtoritajiet. Id-Direttiva wasslet għal progress sostantiv fil-kriminalizzazzjoni tal-attakki ċibernetiċi fuq livell komparabbli fl-Istati Membri kollha, li tiffaċilita l-kooperazzjoni transfruntiera tal-awtoritajiet tal-infurzar tal-liġi li qed jinvestigaw dan it-tip ta' reati. Madankollu, għad hemm kamp ta' applikazzjoni konsiderevoli għad-Direttiva biex tilħaq il-potenzjal sħiħ tagħha jekk l-Istati Membri kellhom jimplimentaw id-dispożizzjonijiet kollha b'mod sħiħ[60]. Il-Kummissjoni se tkompli tipprovdi appoġġ lill-Istati Membri fl-implimentazzjoni tagħhom tad-Direttiva u attwalment ma tarax il-ħtieġa li tipproponi emendi għaliha.

3.1 L-identifikazzjoni ta' atturi malizzjużi

Sabiex jiżdiedu ċ-ċansijiet tagħna li l-awturi jitressqu quddiem il-ġustizzja, għandna bżonn urġenti li ntejbu l-kapaċità tagħna li nidentifikaw lil dawk responsabbli għal attakki ċibernetiċi. Il-kisba ta' informazzjoni utli għal investigazzjonijiet ta' ċiberkriminalità, l-aktar f'forma ta' traċċi diġitali, hija sfida kbira għall-awtoritajiet tal-infurzar tal-liġi. Għalhekk, għandna bżonn inżidu l-kapaċità teknoloġika li ninvestigaw b'mod effettiv, inkluż permezz tat-tisħiħ tal-unità taċ-ċiberkriminalità tal-Europol b'esperti taċ-ċibernetika. L-Europol saret attur ewlieni fl-appoġġ tal-Istati Membri fl-investigazzjonijiet multi-ġurisdizzjonali. Dan għandu jsir ċentru ta' għarfien tal-infurzar tal-liġi tal-Istati Membri dwar investigazzjonijiet online u l-forensika ċibernetika.

Il-prattika mifruxa ta' tqegħid ta' utenti multipli — kultant eluf minnhom — msejsa fuq indirizz IP wieħed jagħmilha teknikament diffiċli ħafna biex tinvestiga mġiba online malizzjuża. Minħabba f'hekkġieli tkun meħtieġa, pereżempju għal reati kriminali serji bħalma hu l-abbuż sesswali tat-tfal, biex tinvestiga għadd kbir ta' utenti sabiex jiġi identifikat attur

[59] Id-Direttiva 2013/40/UE tal-Parlament Ewropew u tal-Kunsill tat-12 ta' Awwissu 2013 dwar attakki kontra s-sistemi tal-informazzjoni.

[60] COM(2017)474.

wieħed malizzjuż. Għalhekk l-UE ser tinkoraġġixxi l-adozzjoni tal-protokoll il-ġdid (IPv6) minħabba li dan jippermetti l-allokazzjoni ta' utent wieħed għal kull indirizz IP, u b'hekk iġġib benefiċċji ċari għall-infurzar tal-liġi u l-investigazzjonijiet tas-sigurtà ċibernetika. Bħala l-ewwel pass biex titħeġġeġ l-adozzjoni ta' din il-miżura, il-Kummissjoni se tintegra r-rekwiżit biex tiċċaqlaq lejn IPv6 fil-politiki kollha tagħha, inklużi r-rekwiżiti fl-akkwist, l-iffinanzjar tal-proġetti u tar-riċerka kif ukoll l-appoġġ materjali ta' taħriġ. Barra minn hekk, l-Istati Membri għandhom jikkunsidraw il-possibbiltà ta' ftehimiet volontarji mal-Fornituri tas-Servizz tal-Internet sabiex jixprunaw l-adozzjoni tal-IPv6.

Il-Belġju qiegħed fuq quddiem fid-dinja[61] *fir-rata għall-adozzjoni tal-IPv6 wkoll bis-saħħa ta' kooperazzjoni pubblika-privata: il-partijiet ikkonċernati rilevanti kkunsidraw li jillimitaw l-użu ta' indirizz IP wieħed għal massimu ta' 16-il utent bħala parti minn miżura ta' awtoregolazzjoni volontarja, li inċentivat it-tranżizzjoni għall-IPv6*[62].

B'mod aktar ġenerali, għandha tiġi promossa aktar ir-responsabbiltà online. Dan ifisser il-promozzjoni ta' miżuri li jipprevjenu l-abbuż ta' ismijiet tad-dominju għad-distribuzzjoni ta' messaġġi mhux mitluba jew attakki *phishing*. Għal dan il-għan, il-Kummissjoni se taħdem biex ittejjeb il-funzjonament u d-disponibbiltà u l-eżattezza tal-informazzjoni fl-Isem tad-Dominju u s-sistemi IP WHOIS[63] f'konformità mal-isforzi tal-Korporazzjoni tal-Internet dwar l-Ismijiet u n-Numri Assenjati[64].

3.2 Intensifikar tar-rispons tal-infurzar tal-liġi

Investigazzjoni u **prosekuzzjoni** effettiva ta' kriminalità bl-użu tal-internet hi deterrent importanti għal min beħsiebu jwettaq attakki ċibernetiċi. Madankollu, il-qafas proċedurali tal-lum jeħtieġ jiġi adattat aħjar fl-era tal-internet[65]. Il-veloċità ta' attakki ċibernetiċi tista' tegħleb il-proċeduri tagħna, kif ukoll toħloq ħtiġijiet partikolari għal kooperazzjoni rapida minn naħa għal oħra tal-fruntieri. Għal dan l-għan, kif imħabbar fl-Aġenda Ewropea dwar is-Sigurtà, il-Kummissjoni kmieni fl-2018 se tressaq proposti biex **tiffaċilita l-aċċess transfruntier għal bażi ta' evidenza elettronika**. B'mod parallel, il-Kummissjoni qed timplimenta miżuri prattiċi biex ittejjeb l-aċċess transfruntier għal evidenza elettronika għall-investigazzjonijiet kriminali, inkluż finanzjament għat-taħriġ dwar il-kooperazzjoni transfruntiera, l-iżvilupp ta' pjattaforma elettronika għall-iskambju ta' informazzjoni fi ħdan l-UE, u l-istandardizzazzjoni ta' formoli użati tal-kooperazzjoni ġudizzjarja bejn l-Istati Membri.

Ostaklu ieħor għal prosekuzzjoni effettiva hija l-proċeduri forensiċi differenti għall-ġbir ta' evidenza elettronika fl-investigazzjonijiet taċ-ċiberkriminalità fl-Istati Membri. Din tista' titnaqqas permezz ta' ħidma lejn it-twaqqif ta' standards forensiċi komuni. Barra minn hekk, għall-appoġġ tat-traċċabbiltà u l-attribwizzjoni, jenħtieġ li jissaħħu l-kapaċitajiet forensiċi. Pass wieħed ikun l-iżvilupp ulterjuri tal-kapaċità forensika eżistenti tal-Europol, l-adattament tar-riżorsi baġitarji u umani fiċ-Ċentru Ewropew taċ-Ċiberkriminalità tal-Europol biex tiġi sodisfatta l-ħtieġa li qed tikber għal appoġġ operazzjonali f'investigazzjonijiet ta'

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

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

[63] Protokoll ta' tfittxija u rispons li jintuża ħafna għat-tiftix ta' bażijiet tad-dejta li jaħżnu l-utenti rreġistrati jew iċ-ċessjonarji ta' riżorsa tal-internet.

[64] Il-Korporazzjoni tal-Internet dwar l-Ismijiet u n-Numri Assenjati (ICANN) hija organizzazzjoni mingħajr skop ta' qligħ responsabbli għall-koordinazzjoni tal-proċeduri ta' manutenzjoni ta' bosta bażijiet tad-dejta relatati mal-ispazji tal-ismijiet tal-internet.

[65] Biex nagħtu eżempju wieħed biss, is-server ċentrali ta' kmand u kontroll (virtwali) tal-botnet Avalanche mexxa servers u dominji fiżiċi kull ħames minuti.

ċiberkriminalità transfruntiera. Pass ieħor għandu jirrifletti l-fokus teknoloġiku stabbilit hawn fuq għal kriptaġġ billi wieħed iħares lejn kif l-abbuż minn kriminali joħloq sfidi sinifikanti fil-ġlieda kontra reati serji, inkluż it-terroriżmu u ċ-ċiberkriminalità. Il-Kummissjoni se tressaq ir-riżultati ta' riflessjonijiet attwali dwar ir-**rwol ta' kriptaġġ fl-investigazzjonijiet kriminali**[66] sa Ottubru 2017[67].

Minħabba n-natura mingħajr fruntieri tal-internet, il-qafas għall-kooperazzjoni internazzjonali pprovdut mill-**Konvenzjoni ta' Budapest dwar iċ-Ċiberkriminalità**[68] tal-Kunsill tal-Ewropa joffri l-opportunità fost grupp divers ta' pajjiżi li jużaw l-istandard legali ottimali għal-leġiżlazzjoni nazzjonali differenti li tindirizza iċ-ċiberkriminalità. Bħalissa qed tiġi esplorata żieda possibbli ta' protokoll għall-Konvenzjoni[69], li tkun tista' tipprovdi wkoll opportunità utli biex tiġi indirizzata l-kwistjoni ta' aċċess transfruntier għal evidenza elettronika f'kuntest internazzjonali. Minflok il-ħolqien ta' strumenti legali internazzjonali ġodda għal kwistjonijiet ta' ċiberkriminalità, l-UE ssejjaħ lill-pajjiżi kollha biex ifasslu leġiżlazzjoni nazzjonali xierqa u jfittxu kooperazzjoni fi ħdan dan il-qafas internazzjonali eżistenti.

Id-disponibbiltà mifruxa ta' għodod ta' anonimizzazzjoni tagħmilha iżjed faċli għall-kriminali biex jinħbew. Id-"**Darknet**"[70] fetaħ toroq ġodda għall-kriminali biex jaċċessaw materjal tal-abbuż sesswali tat-tfal, id-drogi jew l-armi tan-nar, ħafna drabi bi ftit riskju li wieħed jinqabad[71]. Issa huwa wkoll sors ewlieni ta' għodod użati kontra ċ-ċiberkriminalità, bħal malwer u għodod ta' hacking. Il-Kummissjoni, flimkien mal-partijiet interessati rilevanti, se tanalizza l-approċċi nazzjonali bil-ħsieb li jiġu identifikati soluzzjonijiet ġodda. L-Europol għandha tiffaċilita u tappoġġja l-investigazzjonijiet fuq id-darknet, tivvaluta t-theddid u tgħin biex tiddetermina l-ġurisdizzjoni u tagħti prijorità lil każijiet ta' riskju għoli, u li l-UE jista' jkollha rwol ewlieni fil-koordinazzjoni ta' azzjoni internazzjonali[72].

Qasam wieħed tal-attività taċ-ċiberkriminalità li qed jikber huwa l-użu frodulenti ta' dettalji tal-kard tal-kreditu jew mezzi elettroniċi oħra ta' pagament. Kredenzjali ta' pagament miksuba permezz ta' attakki ċibernetiċi kontra l-bejjiegħa bl-imnut fuq l-internet jew xi forma oħra ta' negozji leġittimi mbagħad jiġu negozjati online u jistgħu jintużaw minn kriminali

---

66 Il-Presidenza tal-Kunsill, "L-Eżitu tal-laqgħa tal-Kunsill tal-Ġustizzja u l-Affarijiet Interni tat-8 u d-9 ta' Diċembru 2016", Nru. 15391/16.

67 It-tmien rapport ta' progress lejn Unjoni tas-Sigurtà effettiva u ġenwina tad-29 ta' Ġunju 2017, (COM(2017) 354 final.

68 Il-Konvenzjoni hi l-ewwel trattat internazzjonali dwar reati mwettqa permezz tal-internet u netwerks oħrajn ta' kompjuters, li jittrattaw b'mod partikolari ma' ksur tad-drittijiet tal-awtur, frodi relatata ma' kompjuters, pedopornografija u ksur tas-sigurtà ta' netwerk. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 Fl-2017, 55 gvern irratifika jew issieħeb fil-Konvenzjoni Ewropea dwar iċ-Ċiberkriminalità.

69 It-Termini ta' Referenza għat-tħejjija ta' abbozz tat-tieni Protokoll Addizzjonali għall-Konvenzjoni ta' Budapest dwar iċ-Ċiberkriminalità, T-CY (2017)3.

70 Id-darknet jikkonsisti f'kisja netwerks li jużaw l-internet iżda jeħtieġu softwer , konfigurazzjonijiet jew awtorizzazzjoni speċifiċi għal aċċess. Id-darknet jifforma parti żgħira mill-web profond, il-parti tal-Web mhux indiċjata mill-magni tat-tiftix.

71 Eċċezzjoni notevoli hija t-tneħħija riċenti ta' tnejn mill-akbar swieq tad-dark Web kriminali, AlphaBay u Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 L-Europol diġà għandha rwol importanti f'dan il-qasam. Għal eżempju reċenti ara: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

biex iwettqu frodi[73]. Il-Kummissjoni qed tippreżenta proposta biex tissaħħaħ id-deterrenza permezz ta' **Direttiva dwar il-ġlieda kontra l-frodi u l-iffalsifikar ta' mezzi ta' pagament mhux bi flus kontanti**[74]. Din għandha l-għan li taġġorna r-regoli eżistenti f'dan il-qasam u ssaħħaħ il-kapaċità tal-infurzar tal-liġi biex jindirizzaw dan it-tip ta' reat.

Il-kapaċitajiet investigattivi ċiberkriminali tal-awtoritajiet tal-infurzar tal-liġi tal-Istati Membri jeħtieġu wkoll li jiġu mtejba, kif ukoll l-fehim ta' delitti bl-użu tal-internet u opzjonijiet investigattivi minn prosekuturi u mill-ġudikatura. L-Eurojust u l-Europol jikkontribwixxu għal dan l-objettiv u għal koordinazzjoni msaħħa, f'kooperazzjoni mill-qrib mal-gruppi konsultattivi speċjalizzati fi ħdan iċ-Ċentru kontra ċ-Ċiberkriminalità tal-Europol u man-netwerks tal-kapijiet tal-unitajiet taċ-ċiberkriminalità u ta' prosekuturi speċjalizzati fiċ-ċiberkriminalità. Il-Kummissjoni se tiddedika EUR 10.5 miljun ta' finanzjament għall-ġlieda kontra ċ-ċiberkriminalità, primarjament taħt il-**Programm ta' Fondi għall-Pulizija għas-Sigurtà Interna** tagħha. It-taħriġ huwa element importanti u ġew żviluppati għadd ta' materjali utli mill-Grupp Ewropew għat-Taħriġ u l-Edukazzjoni dwar iċ-Ċiberkriminalità. Dawn issa jridu jiġu implimentati b'mod wiesa' għall-professjonisti tal-infurzar tal-liġi bl-appoġġ tal-Aġenzija tal-Unjoni Ewropea għat-Taħriġ fl-Infurzar tal-Liġi.

3.3 Il-kooperazzjoni pubblika-privata kontra ċ-ċiberkriminalità

L-effikaċja ta' mekkaniżmi ta' nfurzar tal-liġi tradizzjonali hija kkontestata mill-karatteristiċi tad-dinja diġitali, li tikkonsisti l-iktar f'infrastruttura b'sjieda privata u bosta atturi differenti f'diversi ġurisdizzjonijiet. B'riżultat ta' dan, il-kooperazzjoni mas-settur privat, inklużi l-industrija u s-soċjetà ċivili, hija fundamentali għall-awtoritajiet pubbliċi biex tiġi miġġielda l-kriminalità b'mod effettiv. F'dan il-kuntest, is-settur finanzjarju huwa importanti wkoll u għandha tiżdied il-kooperazzjoni. Pereżempju, ir-rwol ta' Unitajiet ta' Intelligence Finanzjarja[75] fil-kuntest taċ-ċiberkriminalità għandu jiġi msaħħaħ.

Xi Stati Membri diġà ħadu passi ewlenin. Fin-Netherlands, l-istituzzjonijiet finanzjarji u l-awtoritajiet tal-infurzar tal-liġi jaħdmu id f'id biex jindirizzaw il-frodi online u ċ-ċiberkriminalità fit-Task Force ta' Kriminalità Elettronika. Iċ-Ċentru ta' Kompetenza Ġermaniża kontra l-Kriminalità Elettronika jipprovdi ċentru operazzjonali għall-membri tiegħu għall-iskambju ta' informazzjoni f'kollaborazzjoni mill-qrib mal-Uffiċċju tal-Pulizija Federali Ġermaniża u jiżviluppa miżuri mmirati biex jiżguraw protezzjoni kontra ċ-ċiberkriminalità. 16-il Stat Membru[76] ħolqu Ċentri ta' Eċċellenza taċ-Ċiberkriminalità biex jiffaċilitaw il-kooperazzjoni bejn l-awtoritajiet tal-infurzar tal-liġi, akkademja u sħab privati għall-iżvilupp u l-iskambju tal-aħjar prattiki, taħriġ u bini tal-kapaċità.

Il-Kummissjoni tappoġġja t-twaqqif ta' sħubijiet pubbliċi-privati u mekkaniżmi ta'

[73] Ir-rikavati tal-frodi huma sors importanti ta' dħul għall-kriminalità organizzata u għalhekk jippermettu t-twettiq ta' attivitajiet kriminali oħrajn bħalma huma t-terroriżmu, it-traffikar tad-drogi u t-traffikar tal-bnedmin.

[74] COM(2017) 489.

[75] L-Unitajiet tal-Intelligence Finanzjarja jservu bħala ċentru nazzjonali għar-riċeviment u l-analiżi ta' rapporti ta' tranżazzjonijiet suspettużi u informazzjoni rilevanti oħra dwar ħasil tal-flus, reati predikati assoċjati u finanzjament tat-terroriżmu, u għat-tixrid tar-riżultati ta' dik l-analiżi.

[76] L-Awstrija, il-Belġju, il-Bulgarija, Ċipru, ir-Repubblika Ċeka, l-Estonja, Franza, il-Ġermanja, il-Greċja, l-Irlanda, il-Litwanja, il-Polonja, ir-Rumanija, is-Slovenja, Spanja u r-Renju Unit.

kooperazzjoni permezz ta' proġetti speċifiċi bħalma huma ċ-Ċentru Ċibernetiku tal-Frodi Online u n-Netwerk ta' Esperti,[77] li jimplimentaw il-mudell tal-kondiviżjoni tal-informazzjoni u standard biex janalizzaw u jimmitigaw ir-riskji ta' frodi online u reati elettroniċi.

Fil-kuntest taċ-ċiberkriminalità, impriżi privati jridu jkunu jistgħu jikkondividu informazzjoni dwar inċidenti konkreti tal-infurzar tal-liġi — inkluża dejta personali — b'rispett sħiħ tar-regoli tal-protezzjoni tad-dejta. Ir-riforma tal-protezzjoni tad-dejta tal-UE, li se tidħol fis-seħħ f'Mejju tal-2018, tipprovdi sett ta' regoli komuni li jistabbilixxi l-kundizzjonijiet li skonthom l-awtoritajiet tal-infurzar tal-liġi u ta' entitajiet privati jistgħu jikkooperaw. Il-Kummissjoni Ewropea se taħdem mal-Bord Ewropew għall-Protezzjoni tad-Dejta u l-partijiet interessati rilevanti biex tidentifika l-aħjar prattiki f'dan il-qasam u, fejn xieraq, tipprovdi gwida.

3.4 Intensifikar tar-rispons politiku

Il-**qafas** adottat reċentement **għal rispons diplomatiku konġunt tal-UE għal attivitajiet malizzjużi ċibernetiċi**[78] (is-"sett ta' għodod taċ-ċiberdiplomazija") jistabbilixxi l-miżuri taħt il-Politika Estera u ta' Sigurtà Komuni, inklużi miżuri restrittivi li jistgħu jintużaw biex tissaħħaħ ir-reazzjoni tal-UE għal attivitajiet li jolqtu l-interessi politiċi, ta' sigurtà u ekonomiċi. Il-qafas jikkostitwixxi pass importanti fl-iżvilupp ta' sinjalar u kapaċitajiet ta' reazzjoni fuq livell tal-UE u tal-Istati Membri. Dan se jżid il-kapaċità tagħna li nattribwixxu attivitajiet ċibernetiċi malizzjużi, bl-għan li jinfluwenzaw l-imġiba ta' aggressuri potenzjali, filwaqt li tiġi kkunsidrata l-ħtieġa li jiġi żgurat rispons proporzjonati. L-attribuzzjoni lil attur Statali jew attur mhux Statali tibqa' d-deċiżjoni politika sovrana bbażata fuq l-intelligence tas-sorsi kollha. Il-ħidma fuq l-implimentazzjoni tal-Qafas attwalment għaddejja ma' Stati Membri u wkoll titmexxa 'l quddiem f'koordinazzjoni mill-qrib mal-Pjan ta' Azzjoni dettaljat għal rispons għal inċidenti ċibernetiċi fuq skala kbira[79]. L-għarfien tas-sitwazzjoni meħtieġa għall-użu ta' miżuri fi ħdan il-qafas għandu jiġu magħqud flimkien, analizzat u kondiviż permezz tal-INTCEN,[80] f'ħidma mill-qrib flimkien mal-Istati Membri u l-istituzzjonijiet tal-UE.

3.5 Bini ta' deterrent taċ-ċibersigurtà permezz tal-kapaċitajiet ta' difiża tal-Istati Membri

L-Istati Membri diġà qed jiżviluppaw kapaċitajiet fil-qasam taċ-ċiberdifiża. Barra minn hekk, minħabba l-ambigwità bejn id-difiża ċibernetika u s-sigurtà ċibernetika u n-natura ta' użu doppju ta' għodod ċibernetiċi u teknoloġiji, kif ukoll differenzi kbar bejn l-approċċi tal-Istati Membri, l-UE tinsab f'pożizzjoni tajba biex tippromwovi sinerġiji bejn l-isforzi militari u dawk ċivili[81].

Dawk l-Istati Membri b'kapaċitajiet aktar avvanzati taċ-ċibersigurtà u li huma lesti biex jiġbruhom flimkien jistgħu jikkunsidraw, bl-appoġġ tar-Rappreżentant Għoli, il-Kummissjoni u l-Aġenzija Ewropea għad-Difiża, biex jinkludu ċ-ċibersigurtà fil-qafas ta' "Kooperazzjoni

---

[77] L-inizjattiva EU-OF2CEN għandha l-għan li tippermetti l-qsim sistematiku u mal-UE kollha ta' informazzjoni relatata ma' frodi tal-internet bejn il-banek u s-servizzi tal-infurzar tal-liġi għall-prevenzjoni ta' pagamenti għal dawk li jwettqu l-frodi u kurrieri ta' flus miksuba illegalment u għall-investigazzjoni u l-prosekuzzjoni tal-awturi involuti. Hija kofinanzjata mill-UE (il-Programm għall-Finanzjament tal-Pulizija għas-Sigurtà Interna).

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

[79] C(2017) 6100.

[80] JOIN(2016) 018 final.

[81] L-UE tifhem l-ispazju ċibernetiku bħala isem ta' dominju ta' operazzjonijiet bħal art, arja u baħar. L-isforzi fil-qasam taċ-ċiberdifiża jinkludu wkoll il-ħarsien u r-reżiljenza ta' assi tal-ispazju u infrastrutturi tal-art relatati.

Strutturata Permanenti" (PESCO). Dan jista' jkun ibbażat fuq il-ħidma msemmija hawn fuq biex tinkoraġġixxi l-kapaċitajiet industrijali u l-awtonomija strateġika tal-UE. L-UE tista' tippromwovi wkoll l-interoperabbiltà, inkluż bl-iffaċilitar tal-iżvilupp tal-kapaċità, il-koordinazzjoni tat-taħriġ u l-edukazzjoni u l-użu doppju ta' sforzi ta' standardizzazzjoni.

Għandu jsir ukoll użu sħiħ tal-qafas konġunt bħala rispons għat-theddid ibridu, li spiss jinvolvi attakki ċibernetiċi, notevolment permezz tal-Ċellola ta' Fużjoni Ibrida tal-UE u ċ-Ċentru Ewropew għall-Ġlieda kontra t-Theddid Ibridu stabbilit riċentement f'Ħelsinki, li l-missjoni tiegħu hu li jinkoraġġixxi djalogu strateġiku u jwettaq riċerka u analiżi.

L-UE ser tagħti enfasi mġedda għall-Qafas tal-Politika għaċ-Ċiberdifiża tal-UE[82], bħala għodda biex tkompli tintegra ċibersigurtà u difiża lejn Politika ta' Sigurtà u ta' Difiża Komuni (PSDK). Iċ-ċiber-reżiljenza tal-missjonijiet u l-operazzjonijiet tal-PSDK stess hi essenzjali: se jiġu żviluppati proċeduri standardizzati u kapaċitajiet tekniċi, li jistgħu jappoġġjaw kemm missjonijiet u operazzjonijiet ċivili u militari skjerati kif ukoll l-istrutturi ta' Kapaċità tal-Ippjanar u t-Tmexxija rispettivi tagħhom u l-forniturі ta' servizzi tat-teknoloġija tal-informazzjoni fis-SEAE. Sabiex isir avvanz fil-kooperazzjoni tal-Istati Membri u jkun hemm gwida aħjar fl-isforzi tal-UE f'dan il-qasam, l-Aġenzija Ewropea għad-Difiża u s-SEAE, b'kooperazzjoni mas-servizzi tal-Kummissjoni, se jiffaċilitaw l-impenn ta' livell strateġiku bejn dawk li jfasslu l-politika taċ-ċiberdifiża tal-Istati Membri. L-UE ser tappoġġja wkoll l-iżvilupp ta' soluzzjonijiet taċ-ċibersigurtà Ewropea bħala parti mill-isforzi tagħha favur Bażi Industrijali u Teknoloġika tad-Difiża Ewropea. Dan jinkludi wkoll it-trawwim ta' raggruppamenti reġjonali ta' eċċellenza taċ-ċibersigurtà u ċ-ċiberdifiża.

Is-servizzi tal-Kummissjoni, filwaqt illi jaħdmu f'kooperazzjoni mill-qrib mas-SEAE, l-Istati Membri u korpi oħra rilevanti tal-UE, ser iqiegħdu fis-seħħ sal-2018 **pjattaforma ta' edukazzjoni u taħriġ fil-qasam taċ-ċiberdifiża** biex tiġi indirizzata d-diskrepanza attwali fil-ħiliet fil-qasam taċ-ċiberdifiża. Dan se jikkumplimenta l-ħidma tal-Aġenzija Ewropea għad-Difiża f'dan il-qasam, billi tindirizza d-diskrepanza attwali fil-ħiliet fil-qasam taċ-ċibersigurtà u ċ-ċiberdifiża.

Azzjonijiet ewlenin

- Inizjattiva tal-Kummissjoni ta' aċċess transfruntier għal evidenza elettronika (kmieni fl-2018);
- L-adozzjoni rapida mill-Parlament Ewropew u l-Kunsill tad-Direttiva proposta dwar il-ġlieda kontra l-frodi u l-iffalsifikar ta' mezzi ta' pagament mhux bi flus kontanti;
- L-introduzzjoni ta' rekwiżiti dwar l-IPv6 fl-akkwisti tal-UE, ir-riċerka u l-finanzjament tal-proġetti; ftehimiet volontarji bejn l-Istati Membri u l-Forniturі tas-Servizz tal-Internet biex jiżdied l-użu tal-IPv6;
- Fokus imġedded/imwessgħa fl-Europol dwar il-forensika ċibernetika u l-monitoraġġ permezz tad-darknet;
- L-implimentazzjoni tal-qafas għal programm konġunt tal-UE bħala rispons diplomatiku għal attivitajiet malizzjużi ċibernetiċi;
- Appoġġ finanzjarju rafforzat għal proġetti nazzjonali u transnazzjonali għat-titjib tal-ġustizzja kriminali fiċ-ċiberspazju.
- Pjattaforma ta' edukazzjoni relatata maċ-ċibersigurtà biex tindirizza d-distakk fil-ħiliet taċ-ċibersigurtà u taċ-ċiberdifiża fl-2018.

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

4. TISĦIĦ TAL-KOOPERAZZJONI INTERNAZZJONALI DWAR IĊ-ĊIBERSIGURTÀ

Iggwidata mill-valuri ewlenin tal-UE u d-drittijiet fundamentali bħal-libertà ta' espressjoni u d-dritt għall-privatezza u l-protezzjoni tad-dejta personali, u l-promozzjoni ta' ċiberspazju miftuħ, ħieles u sikur, il-politika tas-sigurtà ċibernetika internazzjonali tal-UE hija mfassla biex tindirizza l-isfida tal-promozzjoni li kull ma jmur qed tevolvi għall-promozzjoni tal-istabbiltà ċibernetika globali, kif ukoll tikkontribwixxi għall-awtonomija strateġika tal-Ewropa fiċ-ċiberspazju.

4.1 Ċibersigurtà fir-relazzjonijiet esterni

L-evidenza tissuġġerixxi li nies minn madwar id-dinja jidentifikaw attakki ċibernetiċi minn pajjiżi oħra bħala fost l-akbar theddid għas-sigurtà nazzjonali[83]. Minħabba n-natura globali tat-theddid, il-bini u ż-żamma ta' alleanzi u sħubijiet bsaħħithom ma' pajjiżi terzi hija fundamentali għall-prevenzjoni u l-iskoraġġiment ta' attakki ċibernetiċi - li huma dejjem aktar ċentrali għall-istabbiltà u s-sigurtà internazzjonali. L-UE ser tagħti prijorità lill-istabbiliment ta' qafas strateġiku għall-prevenzjoni tal-kunflitti u l-istabbiltà fiċ-ċiberspazju fl-ingaġġi bilaterali, reġjonali, b'multi partijiet interessati u multilaterali.

L-UE tippromwovi bil-qawwa l-pożizzjoni li l-liġi internazzjonali, u b'mod partikolari l-Karta tan-Nazzjonijiet Uniti, tapplika għaċ-ċiberspazju. Bħala komplement għal liġi internazzjonali vinkolanti, l-UE tħaddan normi mhux vinkolanti volontarji, regoli u prinċipji ta' imġiba responsabbli tal-Istat li ġew artikolati permezz tal-Grupp ta' Esperti Governattivi tan-NU[84]; hija tinkoraġġixxi wkoll l-iżvilupp u l-implimentazzjoni ta' miżuri ta' bini ta' fiduċja reġjonali, kemm fl-Organizzazzjoni għas-Sigurtà u l-Kooperazzjoni fl-Ewropa u f'reġjuni oħra.

Fuq livell bilaterali, djalogi ċibernetiċi[85] se jiġu żviluppati ulterjorment u kkumplementati minn sforzi biex jiffaċilitaw il-kooperazzjoni ma' pajjiżi terzi li jsaħħu l-prinċipji ta' diliġenza u responsabbiltà tal-Istat fiċ-ċiberspazju. L-UE għandha tagħti prijorità lil kwistjonijiet ta' sigurtà internazzjonali fiċ-ċiberspazju fl-impenji internazzjonali tagħha, filwaqt li tassigura li ċ-ċibersigurtà ma ssirx skuża għall-protezzjoni tas-suq u l-limitazzjoni tad-drittijiet u l-libertajiet fundamentali, inklużi l-libertà ta' espressjoni u l-aċċess għall-informazzjoni. Approċċ komprensiv għas-sigurtà ċibernetika jirrikjedi r-rispett tad-drittijiet tal-bniedem, u l-UE ser tkompli żżomm il-valuri ewlenin tagħha madwar id-dinja, filwaqt li tibni fuq il-Linji gwida tal-UE dwar id-Drittijiet tal-Bniedem dwar il-libertà fuq l-internet[86]. F'dan ir-rigward l-UE tisħaq dwar l-importanza tal-partijiet interessati kollha involuti fil-governanza tal-internet.

Il-Kummissjoni ressqet ukoll proposta[87] biex timmodernizza l-kontrolli tal-esportazzjoni tal-UE, inkluża l-introduzzjoni ta' kontrolli fuq l-esportazzjoni fuq it-teknoloġiji ta' sorveljanza ċibernetika kritiċi li jistgħu jikkawżaw ksur tad-drittijiet tal-bniedem jew jintużaw b'mod ħażin kontra s-sigurtà tal-UE nnifisha u ser tintensifika d-djalogi ma' pajjiżi terzi biex tippromwovi l-konverġenza globali u l-imġiba responsabbli f'dan il-qasam.

---

83 Stħarriġ dwar l-Attitudnijiet Globali tar-rebbiegħa tal-2017, tal-Pew Research Centre.

84 A/68/98 u A/70/174.

85 F'Settembru 2017, l-UE kellha djalogi ċibernetiċi mal-Istati Uniti, iċ-Ċina, il-Ġappun, ir-Repubblika tal-Korea, u l-Indja.

86 Linji Gwida tal-UE dwar id-Drittijiet tal-Bniedem dwar il-Libertà tal-Espressjoni Online u Offline.

87 COM(2016) 616.

4.2 Il-bini ta' kapaċità għaċ-ċibersigurtà

L-istabbiltà ċibernetika globali tiddependi fuq il-kapaċità lokali u nazzjonali tal-pajjiżi kollha għall-prevenzjoni u r-rispons għal inċidenti ċibernetiċi u l-investigazzjoni u l-prosekuzzjoni ta' każijiet ta' ċiberkriminalità. L-appoġġ għall-isforzi biex tinbena r-reżiljenza nazzjonali f'pajjiżi terzi għandha żżid il-livell ta' ċibersigurtà fid-dinja, b'konsegwenzi pożittivi għall-UE. Il-ġlieda kontra t-theddid ċibernetiku li dejjem qed jevolvi tissuġġerixxi li hemm bżonn ta' taħriġ, sforzi ta' żvilupp għall-politika u l-leġiżlazzjoni, kif ukoll Skwadri ta' Rispons ta' Emerġenza tal-Kompjuters li jaħdmu b'mod effiċjenti u unitajiet taċ-ċiberkriminalità fil-pajjiżi kollha madwar id-dinja.

Mill-2013 'l hawn, l-UE kienet fuq quddiem nett għall-bini ta' kapaċità għaċ-ċibersigurtà internazzjonali u sistematikament tgħaqqad dawn l-isforzi permezz tal-kooperazzjoni tagħha għall-iżvilupp. L-UE ser tkompli tippromovi l-bini tal-kapaċità mudell ibbażat fuq id-drittijiet, f'konformità mal-approċċ Digital4Development[88]. Il-prijoritajiet għall-bini tal-kapaċità ser ikunu fil-viċinat tal-UE u l-pajjiżi li qed jiżviluppaw li qegħdin jesperjenzaw konnettività li qed tikber b'rata mgħaġġla u l-iżvilupp rapidu ta' theddid. L-isforzi tal-UE ser ikunu komplementari għall-aġenda tal-iżvilupp tal-UE fid-dawl tal-Aġenda 2030 għall-Iżvilupp Sostenibbli u għall-isforzi globali għat-tisħiħ tal-kapaċitajiet istituzzjonali.

Sabiex titjieb l-abbiltà tal-UE li timmobilizza l-għarfien espert kollettiv biex issostni din il-bini tal-kapaċità, għandu jitwaqqaf Netwerk għall-Bini ta' Kapaċità Ċibernetika tal-UE, li jiġbor flimkien lill-SEAE, l-awtoritajiet ċibernetiki tal-Istati Membri, l-aġenziji tal-UE, is-servizzi tal-Kummissjoni, l-akkademja u s-soċjetà ċivili. Dwar il-Bini tal-Kapaċità Ċibernetika tal-UE, se jiġu żviluppati linji gwida biex jgħinu fil-provvediment ta' gwida politika u prijoritizzazzjoni aħjar tal-isforzi tal-UE fl-assistenza lil pajjiżi terzi.

L-UE ser taħdem flimkien ma' donaturi oħra f'dan il-qasam sabiex tiġi evitata d-duplikazzjoni tal-isforzi u jiġi ffaċilitat aktar bini ta' kapaċità mmirat f'reġjuni differenti.

4.3 Kooperazzjoni bejn l-UE u n-Nato

Filwaqt li tibni fuq il-progress sostanzjali li diġà sar, l-UE ser tintensifika l-kooperazzjoni bejn l-UE u n-NATO dwar iċ-ċibersigurtà, it-theddid ibridu u d-difiża, kif maħsuba fid-Dikjarazzjoni Konġunta tat-8 ta' Lulju 2016[89]. Il-prijoritajiet jinkludu t-trawwim tal-interoperabbiltà permezz ta' rekwiżiti u standards koerenti fil-qasam taċ-ċiberdifiża, it-tisħiħ tal-kooperazzjoni fuq taħriġ u eżerċizzji, l-armonizzar tar-rekwiżiti tat-taħriġ.

L-UE u n-NATO ser irawmu wkoll il-kooperazzjoni fir-riċerka u l-innovazzjoni fil-qasam taċ-ċiberdifiża, u jibnu fuq l-arranġament tekniku attwali dwar iċ-ċibersigurtà għall-kondiviżjoni tal-informazzjoni bejn il-korpi rispettivi tagħhom taċ-ċibersigurtà[90]. L-isforzi konġunti riċenti dwar il-ġlieda kontra t-theddid ibridu, partikolarment il-kooperazzjoni bejn iċ-Ċellola ta' Fużjoni tal-UE kontra t-Theddid Ibridu u l-Fergħa ta' Analiżi Ibrida tan-NATO għandhom jiġu ingranati aktar biex tissaħħaħ ir-reżiljenza u r-rispons għall-kriżijiet ċibernetiċi. Aktar kooperazzjoni bejn l-UE u n-NATO ser tiġi promossa permezz ta' eżerċizzji tad-difiża ċibernetika, bl-involviment tas-SEAE u entitajiet oħrajn tal-UE u l-kontropartijiet rilevanti tan-NATO, inkluż maċ-Ċentru ta' Eċċellenza fil-qasam taċ-Ċiberdifiża Kooperattiva tan-NATO f'Tallinn. Għall-ewwel darba, in-NATO u l-UE ser iwettqu eżerċizzji paralleli u koordinati b'rispons għal xenarju ibridu man-NATO li tieħu t-tmexxija fl-2017 u l-UE ser

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] Kapaċità ta' Rispons għal Inċidenti relatati mal-Kompjuters CERT-EU u tan-NATO (NCIRC).

tirreċiproka b'mod simili fl-2018. Ir-rapport li jmiss dwar il-kooperazzjoni bejn l-UE u n-NATO, li għandu jitressaq quddiem il-Kunsilli rispettivi f'Diċembru 2017, ser joffri opportunità biex jikkunsidraw il-possibbiltajiet biex ikomplu jespandu l-kooperazzjoni, b'mod partikolari billi jiżguraw mezzi komuni, sikuri u robusti ta' komunikazzjoni bejn l-istituzzjonijiet u l-korpi rilevanti kollha involuti, inklużi l-ENISA.

Azzjonijiet ewlenin

- Avvanz fil-qafas strateġiku għall-prevenzjoni tal-kunflitti u l-istabbiltà fiċ-ċiberspazju;
- L-iżvilupp ta' Bini ta' Kapaċità tan-Netwerk biex jappoġġja l-kapaċità ta' pajjiżi terzi biex jindirizzaw it-theddid ċibernetiku u l-Linji Gwida dwar il-Bini tal-Kapaċità taċ-Ċibersigurtà tal-UE biex jiġu prijoritizzati aħjar l-isforzi tal-UE;
- Kooperazzjoni ulterjuri bejn l-UE u n-NATO, inkluż il-parteċipazzjoni b'mod parallel u kkoordinat f'eżerċizzji u interoperabbiltà msaħħa ta' standards taċ-ċibersigurtà.

5. KONKLUŻJONI

It-thejjija ċibernetika tal-UE hija ta' importanza ċentrali kemm għas-Suq Uniku Diġitali u l-Politika ta' Sigurtà u ta' Difiża. It-titjib taċ-ċibersigurtà Ewropea u l-indirizzar tat-theddid kemm lil objettivi ċivili u militari huwa essenzjali.

Is-Summit Diġitali li jmiss organizzat mill-Presidenza tal-Estonja fid-29 ta' Settembru 2019 jipprovdi opportunità biex nuru determinazzjoni komuni biex npoġġu ċ-ċibersigurtà fil-qalba tal-UE bħala soċjetà diġitali. Bħala parti minn dan l-impenn komuni, il-Kummissjoni tappella lill-Istati Membri biex iwiegħdu kif biħsiebhom jaġixxu fl-oqsma fejn għandhom ir-responsabbiltà primarja. Dan għandu jinkludi t-tisħiħ tas-sigurtà ċibernetika permezz ta':

- Żgurar ta' implimentazzjoni sħiħa u effettiva tad-Direttiva dwar iċ-Ċibersigurtà (NIS) sad-9 ta' Mejju 2018, kif ukoll ir-riżorsi meħtieġa għall-awtoritajiet pubbliċi responsabbli għas-sigurtà ċibernetika biex iwettqu b'mod effettiv il-kompiti tagħhom;
- L-applikazzjoni tal-istess regoli għal amministrazzjonijiet pubbliċi, minħabba r-rwol li għandhom fis-soċjetà u l-ekonomija kollha kemm hi;
- Il-provvista ta' taħriġ relatat maċ-ċibersigurtà fl-amministrazzjoni pubblika;
- Il-prijoritizzazzjoni tal-għarfien ċibernetiku f'kampanji ta' informazzjoni u li jinkludi ċ-ċibersigurtà bħala parti minn kurrikulu akkademiku u ta' taħriġ vokazzjonali;
- L-użu ta' inizjattivi dwar il-"Kooperazzjoni Strutturata Permanenti" (PESCO) u l-Fond Ewropew tad-Difiża biex jiġi appoġġjat l-iżvilupp ta' proġetti fil-qasam taċ-ċiberdifiża.

Din il-Komunikazzjoni Konġunta stabbilixxiet il-kobor tal-isfida, u l-firxa ta' miżuri li l-UE tista' tieħu. Għandna bżonn ta' Ewropa li tkun reżiljenti, li tista' tipproteġi l-poplu tagħha b'mod effettiv billi tantiċipa l-inċidenti ta' ċibersigurtà, bil-bini ta' protezzjoni b'saħħitha tal-istrutturi u l-imġiba tagħha, billi tirkupra malajr minn kwalunkwe attakki ċibernetiċi, u li tiskoraġġixxi lil dawk responsabbli. Din il-Komunikazzjoni tippreżenta miżuri mmirati li jsaħħu aktar l-istrutturi u l-kapaċitajiet taċ-ċibersigurtà tal-UE b'mod koordinat, b'kooperazzjoni sħiħa tal-Istati Membri u d-diversi strutturi tal-UE kkonċernati u li jirrispettaw il-kompetenzi u r-responsabbiltajiet tagħhom. L-implimentazzjoni tagħha se tipprovdi prova ċara li l-UE u l-Istati Membri se jaħdmu flimkien sabiex jistabbilixxu livell ta' ċibersigurtà ugwali għal sfidi dejjem akbar li qed tiffaċċja l-Ewropa llum.