EVROPSKA KOMISIJA

VISOKA PREDSTAVNICA
EVROPSKE UNIJE ZA ZUNANJE
ZADEVE IN VARNOSTNO
POLITIKO

Bruselj, 7.2.2013
JOIN(2013) 1 final

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Strategija Evropske unije za kibernetsko varnost:

odprt, varen in zanesljiv kibernetski prostor

SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

Strategija Evropske unije za kibernetsko varnost:

odprt, varen in zanesljiv kibernetski prostor

1. UVOD

1.1. Ozadje

Internet in kibernetski prostor na splošno zadnjih dvajset let izredno močno vplivata na vse dele družbe. Naše vsakdanje življenje, temeljne pravice, socialni stiki in gospodarstvo so odvisni od brezhibnega delovanja informacijske in komunikacijske tehnologije. Odprt in svoboden kibernetski prostor je po vsem svetu spodbudil politično in socialno vključenost, odpravil ovire med državami, skupnostmi in državljani ter omogočil povezovanje in izmenjavo informacij in idej po vsem svetu;vzpostavil je forum za svobodno izražanje in uveljavljanje temeljnih pravic ter podprl ljudi pri prizadevanju za demokratično in pravičnejšo družbo – najbolj očitno v času arabske pomladi.

Da bi kibernetski prostor ostal odprt in svoboden, bi morali na spletu veljati isti predpisi, načela in vrednote, ki jih EU podpira tudi v nespletnem okolju. Temeljne pravice, demokracijo in pravno državo je treba varovati tudi v kibernetskem prostoru. Naša svoboda in blaginja sta vse bolj odvisni od zanesljivega in inovativnega internetna, ki se bo še naprej razvijal, če bodo inovacije zasebnega sektorja in civilna družba spodbujale njegovo rast. Vendar je za svobodo na spletu potrebna tudi varnost in zaščita. Kibernetski prostor bi moral biti zaščiten pred incidenti, zlonamernimi dejavnostmi in zlorabami; pri zagotavljanju svobodnega in varnega kibernetskega prostora imajo pomembno vlogo vlade. Izpolnjevati morajo več nalog: varovati dostop in odprtost, spoštovati in varovati temeljne pravice na spletu ter ohranjati zanesljivost in interoperabilnost interneta. Vendar je precejšen del kibernetskega prostora v lasti zasebnih podjetij, ki z njim tudi upravljajo, zato je za uspeh vseh pobud na tem področju treba upoštevati vodilno vlogo zasebnega sektorja.

Informacijska in telekomunikacijska tehnologija je postala steber evropske gospodarske rasti in ključen vir, od katerega so odvisni vsi gospodarski sektorji. Podpira zapletene sisteme, ki zagotavljajo delovanje gospodarstva v ključnih sektorjih, kot so finance, zdravstveno varstvo, energija in promet; mnogi poslovni modeli se zanašajo na neprekinjeno dostopnost interneta in nemoteno delovanje informacijskih sistemov.

S polno uveljavitvijo enotnega digitalnega trga bi Evropa lahko povečala BDP za skoraj 500 milijard EUR na leto[1], kar je povprečno 1 000 EUR na osebo. Za uveljavitev novih s tem povezanih tehnologij, vključno z e-plačili, računalništvom v oblaku ali komuniciranjem med napravami[2], je potrebno zaupanje državljanov. Na žalost je raziskava Eurobarometra leta 2012[3] pokazala, da skoraj tretjina Evropejcev ne zaupa uporabi interneta pri bančništvu ali nakupovanju. Velika večina je povedala tudi, da se zaradi pomislekov o varnosti izogiba razkrivanju osebnih podatkov na spletu. V EU je več kot desetina uporabnikov interneta že bila žrtev spletnih prevar.

---

1 http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

2 Na primer rastline z vgrajenimi senzorji, ki škropilnemu sistemu sporočijo, kdaj jih je treba zaliti.

3 Posebna raziskava Eurobarometra 390 o kibernetski varnosti iz leta 2012.

V zadnjih letih se je izkazalo, da digitalizacija po eni strani prinaša velike koristi, po drugi strani pa je digitalno okolje ranljivo. Število namernih ali naključnih kibernetskih incidentov[4] se zaskrbljujoče hitro povečuje, kar bi lahko prekinilo zagotavljanje bistvenih storitev, ki jih imamo za samoumevne – npr. voda, zdravstveno varstvo, elektrika ali mobilne storitve. Groženj je več vrst – od kriminalnih, politično motiviranih, terorističnih ali državno podprtih napadov do naravnih nesreč in nenamernih napak.

Kibernetska kriminaliteta[5], uperjena proti zasebnemu sektorju in posameznikom, že zdaj vpliva na gospodarstvo EU. Kibernetski kriminalci uporabljajo vedno naprednejše metode za vdiranje v informacijske sisteme, krajo ključnih podatkov ali izsiljevanje podjetij. Porast gospodarskega vohunjenja in državno podprtih dejavnosti v kibernetskem prostoru predstavlja novo kategorijo groženj za vlade in podjetja EU.

V državah, ki niso članice EU, se lahko zgodi, da vlade zlorabijo kibernetski prostor za spremljanje in nadzor svojih državljanov. EU se lahko proti temu bori s spodbujanjem svobode in zagotavljanjem spoštovanja temeljnih pravic na spletu.

Zaradi vseh teh dejavnikov so vlade po svetu začele razvijati strategije za kibernetsko varnost in kibernetski prostor obravnavati kot vedno bolj pomembno mednarodno vprašanje. Čas je, da EU okrepi ukrepe na tem področju. Ta predlog za strategijo Evropske unije za kibernetsko varnost, ki sta ga predložila Komisija in visoka predstavnica Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoka predstavnica), predstavlja vizijo EU na tem področju, pojasnjuje vloge in odgovornosti ter določa potrebne ukrepe; temeljni cilj strategije pa je dobra in učinkovita zaščita in spodbujanje pravic državljanov, da bo spletno okolje EU postalo najvarnejše na svetu.

1.2. Načela kibernetske varnosti

Brezmejni in večplastni internet je postal eden od najučinkovitejših instrumentov za svetovni napredek brez vladnega nadzora ali reguliranja. Zasebni sektor bi moral imeti še naprej vodilno vlogo pri razvoju in vsakodnevnem upravljanju interneta, vendar je vse bolj jasno, da so potrebne zahteve glede preglednosti, odgovornosti in varnosti. Ta strategija pojasnjuje načela, ki bi morala usmerjati politiko kibernetske varnosti v EU in na mednarodni ravni.

Temeljne vrednote EU veljajo tako v digitalnem kot fizičnem svetu

Zakoni in predpisi, ki veljajo na drugih področjih našega vsakdana, veljajo tudi v kibernetskem

prostoru.

---

[4] Kibernetska varnost se na splošno nanaša na zaščitne in druge ukrepe, ki se lahko tako na civilnem kot vojaškem področju uporabijo za zaščito kibernetskega prostora pred navedenimi grožnjami, ki so povezane z njegovimi soodvisnimi omrežji in informacijsko infrastrukturo oziroma jih lahko ogrozijo. Pri kibernetski varnosti gre za ohranjanje razpoložljivosti in celovitosti omrežij in infrastrukture ter zaupnosti informacij, ki jih ta omrežja in infrastruktura vsebujejo.

[5] Kibernetska kriminaliteta se na splošno nanaša na vrsto različnih kriminalnih dejavnosti, pri katerih so računalniki in informacijski sistemi osnovno orodje ali glavna tarča. Kibernetska kriminaliteta obsega običajna kazniva dejanja (npr. goljufija, ponarejanje in kraja identitete), kazniva dejanja v zvezi s vsebino (npr. širjenje otroške pornografije na spletu ali spodbujanje k rasnemu sovraštvu) in kazniva dejanja, tipična za računalnike in informacijske sisteme (npr. napadi na informacijske sisteme, ohromitev storitve in zlonamerna programska oprema).

Varstvo temeljnih pravic, svobode izražanja, osebnih podatkov in zasebnosti

Uspešno in učinkovito zagotavljanje kibernetske varnosti je mogoče samo, če temelji na temeljnih pravicah in svoboščinah, določenih v Listini o temeljnih pravicah Evropske unije, ter temeljnih vrednotah EU. Pravic posameznikov pa ni mogoče zagotoviti brez varnih omrežij in sistemov. Vsaka izmenjava informacij za namene kibernetske varnosti bi morala biti v primerih, ko je ogroženo varstvo osebnih podatkov, skladna z zakonodajo EU o varstvu podatkov in v celoti upoštevati pravice posameznikov na tem področju.

Dostop za vse

Če imajo državljani omejen dostop do interneta ali pa ga sploh nimajo in če so digitalno nepismeni, so v slabšem položaju, saj je digitalizacija prodrla v vse pore družbe. Vsakdo bi moral imeti dostop do interneta in neoviranega pretoka informacij. Zagotoviti je treba celovitost in varnost interneta, da se omogoči varen dostop za vse.

Demokratično in učinkovito upravljanje, ki vključuje več zainteresiranih strani

Digitalnega sveta ne nadzoruje en sam subjekt. Trenutno je v vsakodnevno upravljanje internetnih virov, protokolov in standardov ter v prihodnji razvoj interneta vključenih več zainteresiranih strani, od katerih so mnoge komercialni in nevladni subjekti. EU ponovno poudarja pomen vseh zainteresiranih strani v trenutnem modelu upravljanja interneta in podpira pristop upravljanja, ki vključuje več zainteresiranih strani[6].

Skupna odgovornost za zagotavljanje varnosti

Vedno večja odvisnost od IKT na vseh področjih človekovega življenja je povzročila ranljivosti, ki jih je treba ustrezno opredeliti, podrobno analizirati in odpraviti ali zmanjšati. Vsi zadevni akterji, tako javni organi kot zasebni sektor in posamezni državljani, se morajo za povečanje kibernetske varnosti zavedati skupne odgovornosti, sprejeti ukrepe za lastno zaščito in po potrebi zagotoviti usklajeno odzivanje.

2. STRATEŠKE PREDNOSTNE NALOGE IN UKREPI

EU bi morala zaščititi spletno okolje in zagotoviti najvišjo možno raven svobode in varnosti za vse. Čeprav se Komisija zaveda, da je spopadanje z varnostnimi izzivi v kibernetskem prostoru predvsem naloga držav članic, v tej strategiji predlaga posebne ukrepe, ki lahko povečajo skupno uspešnost EU. Gre za kratkoročne in dolgoročne ukrepe, ki vključujejo raznovrstna orodja politike[7] in različne akterje, od institucij EU in držav članic do industrijskih sektorjev.

Vizija EU, predstavljena v tej strategiji, se za soočanje z zgoraj opisanimi izzivi osredotoča na pet strateških prednostnih nalog:

- zagotavljanje kibernetske odpornosti,
- občutno zmanjšanje kibernetske kriminalitete,

[6] Glej tudi COM(2009) 277, Sporočilo Komisije Evropskemu parlamentu in Svetu „Upravljanje interneta: naslednji koraki“.

[7] Ukrepi, povezani z izmenjavo informacij, ko je ogroženo varstvo osebnih podatkov, bi morali biti skladni z zakonodajo EU o varstvu podatkov.

- oblikovanje politike za kibernetsko obrambo in gradnja zmogljivosti, povezanih s skupno varnostno in obrambno politiko,
- razvoj industrijskih in tehnoloških zmogljivosti za kibernetsko varnost,
- oblikovanje usklajene mednarodne kibernetske politike Evropske unije in spodbujanje temeljnih vrednot EU.

2.1. Zagotavljanje kibernetske odpornosti

Za spodbujanje kibernetske odpornosti v EU morajo javni organi in zasebni sektor graditi zmogljivosti in učinkovito sodelovati. Na podlagi pozitivnih rezultatov, doseženih z do zdaj izvedenimi ukrepi[8], bi lahko nadaljnji ukrepi EU pomagali zlasti pri boju proti kibernetskim tveganjem in grožnjam čezmejnih razsežnosti ter prispevali k usklajenemu odzivu v nujnih primerih. S tem bi zagotovili močno podporo za dobro delovanje notranjega trga in okrepili notranjo varnost EU.

Če si Evropa ne bo močno prizadevala za izboljšanje javnih in zasebnih zmogljivosti, virov in postopkov za preprečevanje, odkrivanje in obravnavanje kibernetskih incidentov, bo ostala ranljiva. Zato je Komisija razvila politiko na področju varnosti omrežij in informacij (v nadaljnjem besedilu: VOI)[9]. **Evropska agencija za varnost omrežij in informacij (ENISA)** je bila ustanovljena leta 2004[10]; Svet in Parlament razpravljata o novi uredbi za okrepitev ENISA in posodobitev njenega mandata[11]. Poleg tega okvirna direktiva o elektronskih komunikacijah[12] od ponudnikov elektronskih komunikacij zahteva, da za varnost svojih omrežij sprejmejo ustrezne ukrepe za obvladovanje tveganj in priglasijo pomembne kršitve varnosti. Prav tako morajo upravljavci podatkov po zakonodaji EU o varstvu podatkov[13] sprejeti varnostne zahteve in ukrepe za varstvo podatkov, upravljavci javno dostopnih storitev e-komunikacij pa morajo pristojnim nacionalnim organom priglasiti incidente, ki vključujejo kršitev varnosti osebnih podatkov.

Kljub napredku, ki so ga prinesle prostovoljne zaveze, v EU še vedno ostajajo vrzeli, zlasti glede nacionalnih zmogljivosti, usklajevanja v primeru čezmejnih incidentov ter vključenosti in pripravljenosti zasebnega sektorja. To strategijo spremlja **zakonodajni** predlog, ki ima predvsem naslednje cilje:

- določitev skupnih minimalnih zahtev za VOI na nacionalni ravni, ki bodo države članice obvezovale, da: imenujejo nacionalne organe, pristojne za VOI, vzpostavijo dobro delujoče skupine za odzivanje na računalniške grožnje (CERT) in sprejmejo nacionalno strategijo za VOI in nacionalni načrt sodelovanja na področju VOI. Gradnja zmogljivosti in usklajevanje zadevajo tudi institucije EU: leta 2012 je bila ustanovljena stalna skupina

---

8 Glej navedbe v tem sporočilu in v delovnem dokumentu služb Komisije o oceni učinka, priloženemu predlogu Komisije za direktivo o varnosti omrežij in informacij, zlasti oddelka 4.1.4 in 5.2 ter priloge 2, 6 in 8.

9 Leta 2001 je Komisija sprejela sporočilo „Varnost omrežij in informacij: predlog evropske politike pristopa“ (COM (2001) 298), leta 2006 pa strategijo za varno informacijsko družbo (COM(2006) 251). Od leta 2009 je Komisija sprejela tudi akcijski načrt in sporočilo o zaščiti kritične evropske infrastrukture (COM(2009) 149), ki sta bila potrjena z Resolucijo Sveta 2009/C 321/01, ter sporočilo o zaščiti kritične informacijske infrastrukture (COM(2011) 163), ki je bilo potrjeno s Sklepi Sveta 10299/11.

10 Uredba (ES) št. 460/2004.

11 COM(2010) 521. Ukrepi, predlagani v tej strategiji, ne pomenijo spremembe veljavnega ali prihodnjega mandata ENISA.

12 Člen 13a in b Direktive 2002/21/ES.

13 Člen 17 Direktive 95/46/ES in člen 4 Direktive 2002/58/ES.

za odzivanje na računalniške grožnje, odgovorna za varnost sistemov IT v institucijah, agencijah in organih EU (CERT-EU);

- vzpostavitev mehanizmov za usklajeno preprečevanje, odkrivanje, ublažitev in odzivanje, ki bodo omogočali izmenjavo informacij in medsebojno pomoč med nacionalnimi organi, pristojnimi za VOI. Nacionalnimi organi, pristojni za VOI, bodo pozvani, naj zagotovijo ustrezno sodelovanje na ravni EU, zlasti na podlagi načrta sodelovanja Unije na področju VOI, oblikovanega za odzivanje na kibernetske incidente s čezmejno razsežnostjo. To sodelovanje bo temeljilo tudi na napredku, doseženem v evropskem forumu za države članice (EFMS)[14], v okviru katerega so potekale plodne razprave in izmenjave izkušenj o javnem redu na področju VOI in ki bo lahko vključen v mehanizem za sodelovanje, ko bo ta vzpostavljen;
- izboljšanje pripravljenosti in vključenosti zasebnega sektorja. Ker je večina omrežij in informacijskih sistemov v zasebni lasti in jih upravljajo zasebna podjetja, je izboljšanje sodelovanja z zasebnim sektorjem ključnega pomena za spodbujanje kibernetske varnosti. Zasebni sektor bi moral na razviti lastno tehnično zmogljivost za kibernetsko odpornost in si med sektorji izmenjati najboljše prakse. Orodja, ki jih je industrija razvila za odzivanje na incidente, ugotavljanje vzrokov in opravljanje forenzičnih preiskav, bi moral izkoristiti tudi javni sektor.

Vendar v zasebnem sektorju še vedno primanjkuje učinkovitih spodbud za zagotavljanje zanesljivih podatkov o obstoju ali vplivu incidentov na področju VOI, za vzpostavitev kulture obvladovanja tveganja in vlaganje v varnostne rešitve. Cilj predlagane zakonodaje je zato zagotoviti, da akterji na številnih ključnih področjih (energetika, promet, bančništvo, borze, ponudniki ključnih internetnih storitev ter javne uprave) ocenijo tveganja na področju kibernetske varnosti, s katerimi se soočajo, z ustreznimi ukrepi za obvladovanje tveganja zagotovijo zanesljivost in odpornost omrežij in informacijskih sistemov in si izmenjujejo informacije z nacionalnimi organi, pristojnimi za VOI. Vzpostavitev kulture kibernetske varnosti bi lahko okrepila poslovne priložnosti in konkurenčnost v zasebnem sektorju, ki bi kibernetsko varnost lahko izkoristil za promoviranje izdelkov in storitev.

Ti subjekti bi morali nacionalnim organom, pristojnim za VOI, priglasiti incidente z znatnim vplivom na neprekinjenost ključnih storitev in dobavo blaga, ki sta odvisni od omrežij in informacijskih sistemov.

Nacionalni organi, pristojni za VOI, bi morali sodelovati z drugimi regulativnimi organi in zlasti z organi za varstvo osebnih podatkov ter si z njimi izmenjevati informacije. Organi, pristojni za VOI, pa bi morali organom kazenskega pregona priglasiti incidente, za katere sumijo, da so resne kriminalne narave. Nacionalni pristojni organi bi morali na posebni spletni strani tudi redno objavljati nezaupne informacije o tekočih zgodnjih opozorilih o incidentih in tveganjih ter o usklajenih odzivih nanje. Pravne obveznosti ne bi smele nadomestiti ali preprečiti oblikovanja neformalnega in prostovoljnega sodelovanja, tudi med javnim in zasebnim sektorjem, za izboljšanje ravni varnosti ter izmenjavo informacij in najboljše prakse. Zlasti evropsko javno-zasebno partnerstvo za odpornost (EP3R)[15] je trdna in ustrezna platforma na ravni EU in bi ga bilo treba še naprej razvijati.

---

[14] Evropski forum za države članice je bil vzpostavljen s sporočilom o zaščiti kritične informacijske infrastrukture (COM(2009) 149) in je platforma za pospeševanje razprav med javnimi organi držav članic o dobri praksi na področju varnosti in odpornosti kritične informacijske infrastrukture.

[15] Evropsko javno-zasebno partnerstvo za odpornost je bilo ustanovljeno s sporočilom o zaščiti kritične informacijske infrastrukture (COM(2009) 149). V okviru te platforme se je začelo delo in spodbudilo sodelovanje med javnim in zasebnim sektorjem pri določanju ključnih sredstev, virov, funkcij in

Instrument za povezovanje Evrope (IPE)[16] bi zagotovil finančno podporo za ključno infrastrukturo ter tako povezal zmogljivosti držav članic na področju VOI in omogočil lažje sodelovanje po vsej EU.

Poleg tega so vaje na področju kibernetskih incidentov na ravni EU bistvene za simulacijo sodelovanja med državami članicami in zasebnim sektorjem. Prva vaja, ki so se je udeležile države članice, je bila opravljena leta 2010 („Cyber Europe 2010“), druga, ki je vključevala tudi zasebni sektor, pa oktobra 2012 („Cyber Europe 2012“). Simulacijska vaja med EU in ZDA je bila opravljena novembra 2011 („Cyber Atlantic 2011“). Za prihodnja leta so načrtovane nove vaje, tudi na mednarodni ravni.

Komisija bo:

- nadaljevala dejavnosti, ki jih v tesnem sodelovanju z organi držav članic ter lastniki in upravljavci kritične infrastrukture izvaja v okviru Skupnega raziskovalnega središča, za opredelitev ranljivosti evropske kritične infrastrukture na področju VOI ter spodbujanje razvoja odpornih sistemov;
- zgodaj leta 2013 začela pilotni projekt[17] za **boj proti botnetom in zlonamerni programski opremi**, ki ga financira EU, da bi zagotovila okvir za usklajevanje in sodelovanje med državami članicami EU, organizacijami zasebnega sektorja, kot so ponudniki internetnih storitev, in mednarodnimi partnerji.

Komisija poziva ENISA, naj:

- državam članicam pomaga razviti močne **nacionalne zmogljivosti za kibernetsko odpornost**, zlasti z gradnjo kompetenc na področju varnosti in odpornosti industrijskih krmilnih sistemov ter prometne in energetske infrastrukture;
- leta 2013 pregleda možnost oblikovanja skupin za odzivanje na računalniške varnostne incidente na področju industrijskih krmilnih sistemov v EU;
- še naprej podpira države članice in institucije EU pri opravljanju rednih **vseevropskih vaj na področju kibernetskih incidentov**, ki bodo tudi operativna podlaga za sodelovanje EU v mednarodnih vajah na področju kibernetskih incidentov.

Komisija poziva Evropski parlament in Svet, naj:

- hitro sprejmeta predlog direktive o **skupni visoki ravni varnosti omrežij in informacij** v Uniji, ki obravnava nacionalne zmogljivosti in pripravljenost, sodelovanje na ravni EU, vzpostavitev kulture obvladovanja tveganja in izmenjevanje informacij o VOI.

Komisija poziva industrijo, naj:

---

temeljnih zahtev za odpornost ter potreb po sodelovanju in mehanizmih za odzivanje na obsežne prekinitve, ki vplivajo na elektronske komunikacije.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Proračunska vrstica 09.03.02 IPE–telekomunikacijska omrežja (spodbujanje medsebojnega povezovanja in interoperabilnosti nacionalnih javnih storitev na spletu in dostopa do takih omrežij).

17 CIP-ICT-PSP-2012-6, 325188. Skupni proračun je 15 milijonov EUR, financiranje EU pa znaša 7,7 milijona EUR.

18 http://www.trustindigitallife.eu/.

prevzame vodilno vlogo pri **vlaganju** v visoko raven kibernetske varnosti ter spodbuja izmenjavo najboljše prakse in informacij znotraj sektorja in z javnimi organi, da bo zagotovila močno in učinkovito zaščito sredstev in posameznikov, zlasti z javno-zasebnimi partnerstvi, kot sta EP3R in Trust in Digital Life (Zaupanje v digitalno življenje)[18].

Ozaveščanje

Zagotavljanje kibernetske varnosti je odgovornost vseh. Končni uporabniki imajo ključno vlogo pri zagotavljanju varnosti omrežij in informacijskih sistemov: treba jih je osvestiti o tveganjih, s katerimi se soočajo na spletu, in jim dati možnost, da sprejemajo preproste ukrepe za obrambo.

V zadnjih letih je bilo razvitih več pobud, ki bi jih bilo treba nadaljevati. Zlasti ENISA je z objavljanjem poročil, organiziranjem strokovnih delavnic in razvijanjem javno-zasebnih partnerstev prispevala k izboljšanju ozaveščenosti. Europol, Eurojust in nacionalni organi za varstvo podatkov so prav tako dejavni na tem področju. Oktobra 2012 je ENISA skupaj z nekaterimi državami članicami poskusno organizirala „evropski mesec kibernetske varnosti“. Ozaveščanje je eno od področij delovne skupine EU–ZDA za kibernetsko varnost in kibernetsko kriminaliteto[19] in ima pomembno vlogo tudi v okviru programa Varnejši internet[20], ki se osredotoča na varnost otrok na spletu.

Komisija poziva ENISA, naj:

- leta 2013 predlaga časovni načrt za „vozniško dovoljenje za varnost omrežij in informacij“ (program za prostovoljno certificiranje, ki spodbuja izboljševanje spretnosti in kompetenc strokovnjakov na področju IT, npr. skrbnikov spletišč).

Komisija bo:

- ob podpori ENISA leta 2014 organizirala **prvenstvo** kibernetske varnosti, na katerem bodo univerzitetni študenti tekmovali s predlogi za rešitve na področju VOI.

Komisija poziva države članice[21], naj:

- s pomočjo ENISA in ob sodelovanju zasebnega sektorja od leta 2013 naprej vsako leto organizirajo **mesec kibernetske varnosti**, da se poveča ozaveščenost končnih uporabnikov. Leta 2014 bo mesec kibernetske varnosti organiziran vzporedno v EU in ZDA;
- **okrepijo nacionalna prizadevanja za izobraževanje in usposabljanje na področju VOI** z uvedbo: usposabljanja na področju VOI v šolah do leta 2014, usposabljanja na področju VOI, razvoja programske opreme in varstva osebnih podatkov za študente računalništva in osnovnega usposabljanja na področju VOI za zaposlene v javnih upravah.

19 Naloga te delovne skupine, ustanovljene na vrhu EU-ZDA novembra 2010 (MEMO/10/597), je razvoj skupnih pristopov k najrazličnejšim vprašanjem na področju kibernetske varnosti in kriminalitete.

20 V okviru programa za varnejši internet se financira mreža nevladnih organizacij, ki delujejo na področju zaščite otrok na spletu, mreža organov pregona, ki si izmenjujejo informacije in najboljše prakse v zvezi s kazenskimi zlorabami interneta za razširjanje gradiva o spolni zlorabi otrok, in mreža raziskovalcev, ki zbirajo informacije o uporabi, tveganjih in posledicah spletnih tehnologij za življenje otrok.

21 Tudi z vključevanjem ustreznih nacionalnih organov, vključno z organi, pristojnimi za VOI, in organi za varstvo podatkov.

Komisija poziva industrijo, naj:

- spodbuja **ozaveščenost** o kibernetski varnosti **na vseh ravneh**, tako v poslovnih praksah kot v stikih z uporabniki. Industrija bi morala zlasti razmisliti o načinih, kako povečati odgovornost izvršnih direktorjev in uprav za zagotavljanje kibernetske varnosti.

2.2. Občutno zmanjšanje kibernetske kriminalitete

Večja digitalizacija sveta pomeni več možnosti za kibernetske kriminalce. Kibernetska kriminaliteta je ena od najhitreje rastočih oblik kriminala, saj vsak dan prizadene več kot milijon ljudi po vsem svetu. Kibernetski kriminalci uporabljajo vse naprednejše tehnike, njihove mreže pa so vse bolj razvite, zato za spopadanje z njimi potrebujemo prava operativna orodja in zmogljivosti. Kibernetska kriminaliteta prinaša visoke dobičke ob nizkem tveganju, saj kriminalci pogosto izkoristijo anonimnost spletnih domen. Kibernetska kriminaliteta ne pozna meja – svetovna razsežnost interneta pomeni, da morajo organi kazenskega pregona sprejeti usklajen in skupen čezmejni pristop k odzivanju na to vse večjo grožnjo.

Trdna in učinkovita zakonodaja

EU in države članice za boj proti kibernetski kriminaliteti potrebujejo trdno in učinkovito zakonodajo. Konvencija Sveta Evrope o kibernetski kriminaliteti, podpisana v Budimpešti, je zavezujoča mednarodna pogodba, ki zagotavlja učinkovit okvir za sprejemanje nacionalne zakonodaje.

EU je že sprejela zakonodajo o kibernetski kriminaliteti, vključno z direktivo o boju proti spolnemu izkoriščanju otrok na spletu in otroški pornografiji[22]. EU bo sprejela tudi direktivo o napadih na informacijske sisteme, zlasti z uporabo botnetov.

Komisija bo:

- zagotovila hiter prenos in izvajanje direktiv, povezanih s kibernetsko kriminaliteto;
- tiste države članice, ki še niso ratificirale **konvencije Sveta Evrope o kibernetski kriminaliteti**, pozvala, naj to storijo čim prej in začnejo izvajati njene določbe.

Izboljšana operativna zmogljivost za boj proti kibernetski kriminaliteti

Metode kibernetske kriminalitete se zelo hitro razvijajo, zato se organi kazenskega pregona proti njej ne morejo boriti z zastarelimi operativnimi orodji. Trenutno nekatere države članice EU še nimajo operativne zmogljivosti, ki jo potrebujejo za učinkovito odzivanje na področju kibernetske kriminalitete. Vse države članice potrebujejo učinkovite nacionalne enote za kibernetsko kriminaliteto.

[22] Direktiva 2011/93/EU o nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ.

Komisija bo:

- s programi financiranja[23] podpirala države članice, da **opredelijo vrzeli in okrepijo svojo zmogljivost** za preiskovanje kibernetske kriminalitete in boj proti njej. Poleg tega bo podpirala organe, ki povezujejo raziskovalni in akademski svet, strokovnjake, ki delujejo na področju kazenskega pregona, in zasebni sektor; gre za dejavnost, ki je podobna delu, ki ga zdaj opravljajo ponekod že ustanovljeni centri odličnosti za boj proti kibernetski kriminaliteti, financirani s strani Komisije;
- skupaj z državami članicami in ob podpori Skupnega raziskovalnega središča usklajevala prizadevanja za opredelitev najboljših praks in najboljših razpoložljivih tehnik za boj proti kibernetskemu kriminalu (npr. v zvezi z razvojem in uporabo forenzičnih orodij ali analizo groženj);
- tesno sodelovala z nedavno ustanovljenim **Europolovim Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) in z Eurojustom,** da bo politične pristope uskladila z najboljšimi praksami na operativnem področju.

Izboljšano usklajevanje na ravni EU

EU lahko dopolnjuje dejavnosti držav članic tako, da omogoča lažje usklajevanje in sodelovanje ter združuje organe kazenskega pregona in pravosodne organe z javnimi in zasebnimi interesnimi skupinami iz EU in izven nje.

Komisija bo:

- podpirala nedavno ustanovljeni **Evropski center za boj proti kibernetski kriminaliteti** (EC3), ki je evropsko središče za boj proti kibernetski kriminaliteti. EC3 bo zagotavljal analize in podatke, podpiral preiskave, opravljal visokokakovostno forenzično delo, spodbujal sodelovanje, omogočal izmenjavo informacij med pristojnimi organi držav članic, zasebnim sektorjem in drugimi zainteresiranimi stranmi ter postopno postal glasnik organov kazenskega pregona[24];
- v skladu z zakonodajo EU (vključno s pravili o varstvu podatkov) podpirala prizadevanja za povečanje odgovornosti služb za registracijo domenskih imen in zagotovila točnost informacij o lastnikih spletišča, pri čemer se bo zlasti oprla na priporočila na področju kazenskega pregona za organizacijo za dodeljevanje spletnih imen in številk (ICANN);
- na podlagi najnovejše zakonodaje še naprej krepila prizadevanja EU za boj proti spolni zlorabi otrok na spletu. Komisija je sprejela evropsko strategijo za boljši internet za otroke[25] in je skupaj z državami EU in tretjimi državami sklenila

[23] Za leto 2013 v okviru programa Preprečevanje kriminala in boj proti njemu (ISEC). Po letu 2013 v okviru Sklada za notranjo varnost (nov instrument večletnega finančnega okvira).

[24] Evropska komisija je 28. marca 2012 sprejela sporočilo „Boj proti kriminalu v digitalni dobi: ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti“.

[25] COM(2012) 196 final.

svetovno zavezništvo proti spolni zlorabi otrok na internetu[26]. Zavezništvo je forum za nadaljnje ukrepe držav članic, ki jih podpirata Komisija in Evropski center za boj proti kibernetski kriminaliteti.

Komisija poziva Europol (EC3), naj:

- svojo analitično in operativno podporo najprej usmeri k preiskavam kibernetske kriminalitete v državah članicah, da pomaga razbiti in prekiniti mreže kibernetske kriminalitete, zlasti na področju spolne zlorabe otrok, goljufij v zvezi s plačili, botnetov in vdorov;
- redno pripravlja strateška in operativna poročila o trendih in novih grožnjah, da se opredelijo prednostne naloge in da bodo skupine za boj proti kibernetski kriminaliteti v državah članicah lahko izvajale usmerjene preiskave.

Komisija poziva Evropsko policijsko akademijo (CEPOL), naj v sodelovanju z Europolom:

- usklajuje oblikovanje in načrtovanje programov usposabljanja, da bodo organi kazenskega pregona imeli strokovno znanje za učinkovit boj proti kibernetski kriminaliteti.

Komisija poziva Eurojust, naj:

- opredeli glavne ovire za pravosodno sodelovanje na področju preiskav kibernetske kriminalitete in usklajevanje med državami članicami in s tretjimi državami ter podpira preiskovanje in pregon kibernetske kriminalitete tako na operativni kot na strateški ravni in usposabljanje na terenu.

Komisija poziva Eurojust in Europol (EC3), naj:

- tesno sodelujeta, med drugim z izmenjavo informacij, da bosta v skladu s svojim mandatom in pristojnostmi še učinkovitejša pri boju proti kibernetski kriminaliteti.

2.3. Oblikovanje politike za kibernetsko obrambo in gradnja zmogljivosti, povezanih s skupno varnostno in obrambno politiko

Prizadevanja za kibernetsko varnost v EU vključujejo tudi kibernetsko obrambo. Za povečanje odpornosti komunikacijskih in informacijskih sistemov, ki podpirajo interese držav članic na področju obrambe in nacionalne varnosti, bi se moral razvoj zmogljivosti za kibernetsko obrambo osredotočati na odkrivanje naprednih kibernetskih groženj, odzivanje nanje in obnovo po njihovi odpravi.

Glede na to, da so grožnje večplastne, bi bilo treba okrepiti sinergije med civilnimi in vojaškimi pristopi k varovanju ključnih kibernetskih sredstev. Ta prizadevanja bi morala biti podprta z raziskavami in razvojem ter tesnejšim sodelovanjem med vladami, zasebnim sektorjem in akademskim svetom v EU. Da se prepreči podvajanje, bo EU preučila možnosti,

[26] Sklepi Sveta o svetovnem zavezništvo proti spolni zlorabi otrok na internetu (skupna izjava EU in ZDA) z dne 7. in 8. junija 2012 in Deklaracija o ustanovitvi svetovnega zavezništva prot spolni zlorabi otrok na internetu (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm).

kako bi EU in NATO lahko med seboj dopolnjevala prizadevanja za izboljšanje odpornosti ključne vladne, obrambne in druge informacijske infrastrukture, od katere so odvisne članice obeh organizacij.

Visoka predstavnica se bo osredotočila na naslednje ključne dejavnosti ter države članice in Evropsko obrambno agencijo pozvala, naj skupaj:

- ocenijo operativne zahteve za kibernetsko obrambo EU ter spodbujajo razvoj zmogljivosti in tehnologij EU za kibernetsko obrambo, pri čemer je treba obravnavati vse vidike gradnje zmogljivosti, vključno z načeli, vodstvom, organizacijo, osebjem, usposabljanjem, tehnologijo, infrastrukturo, logistiko in interoperabilnostjo;

- oblikujejo okvir EU za politiko kibernetske obrambe, ki bo ščitil omrežja v okviru misij in operacij skupne varnostne in obrambne politike, vključno z dinamičnim obvladovanjem tveganja, izboljšano analizo nevarnosti in izmenjavo informacij; izboljšajo možnosti vojske za usposabljanje in vaje na področju kibernetske obrambe v evropskem in večnacionalnem okviru, tudi z vključitvijo elementov kibernetske obrambe v obstoječe kataloge vaj;

- spodbujajo dialog in usklajevanje med civilnimi in vojaškimi akterji v EU, s posebnim poudarkom na izmenjavi dobrih praks in informacij, zgodnjem opozarjanju, odzivanju na incidente, oceni tveganja, ozaveščanju in določitvi kibernetske varnosti kot prednostne naloge;

- zagotavljajo dialog z mednarodnimi partnerji, vključno z Natom, drugimi mednarodnimi organizacijami in mednarodnimi centri odličnosti, da se zagotovi učinkovita obramba, opredeli področja za sodelovanje in prepreči podvajanje ukrepov.

2.4. Razvoj industrijskih in tehnoloških virov za kibernetsko varnost

Evropa ima odlične zmogljivosti za raziskave in razvoj, vendar imajo številni vodilni svetovni ponudniki inovativnih izdelkov in storitev IKT sedež izven EU. Obstaja tveganje, da Evropa postane preveč odvisna od IKT in varnostnih rešitev, razvitih zunaj svojih meja. Ključno je, da so elementi strojne in programske opreme, proizvedeni v EU ali tretjih državah, ki se uporabljajo v kritičnih storitvah in infrastrukturi, vse bolj pa tudi v mobilnih napravah, zanesljivi in varni ter zagotavljajo varstvo osebnih podatkov.

Spodbujanje enotnega trga izdelkov za kibernetsko varnost

Visoko raven varnosti je mogoče zagotoviti samo, če bodo vsi člani v vrednostni verigi (npr. proizvajalci opreme, razvijalci programske opreme, ponudniki storitev informacijske družbe) varnost določili kot prednostno nalogo. Vendar se zdi[27], da številni akterji varnost še vedno vidijo le kot dodatno breme, povpraševanje po varnostnih rešitvah pa je majhno. Za celotno vrednostno verigo izdelkov IKT, ki se uporabljajo v Evropi, morajo veljati primerne zahteve glede kibernetske varnosti. Zasebni sektor potrebuje spodbude za zagotovitev visoke ravni kibernetske varnosti; na primer, oznake z navedbo o ustrezni kibernetski varnosti bi podjetjem z visoko kibernetsko varnostjo in dobrimi rezultati omogočile, da s tem promovirajo svoje izdelke in storitve ter pridobijo konkurenčno prednost. Poleg tega bi obveznosti, določene v

[27] Glej delovni dokument služb Komisije o oceni učinka, ki je priložen predlogu Komisije za direktivo o varnosti omrežij in informacij, oddelek 4.1.5.2.

predlagani direktivi o VOI, znatno prispevale k okrepitvi konkurenčnosti podjetij v zadevnih sektorjih.

Prav tako bi bilo treba spodbujati povpraševanje po zelo varnih izdelkih na vseevropskem trgu. Ta strategija si prizadeva povečati sodelovanje in preglednost na področju varnosti izdelkov IKT. Poziva k vzpostavitvi platforme za povezovanje ustreznih evropskih javnih in zasebnih zainteresiranih strani, s katero bi opredelili dobre prakse na področju kibernetske varnosti v celotni vrednosti verigi in ustvarili ugodne tržne pogoje za razvoj in sprejetje varnih rešitev IKT. Zelo pomembno je, da se ustvarijo spodbude za izvedbo primernih ukrepov za obvladovanje tveganja ter sprejetje varnostnih standardov in rešitev, poleg tega pa morebiti vzpostavijo tudi prostovoljne sheme certificiranja na ravni EU, ki bi temeljile na obstoječih shemah v EU in na mednarodni ravni. Komisija bo spodbujala sprejetje usklajenih pristopov med državami članicami, da se odpravijo razlike, zaradi katerih so podjetja ponekod lahko v slabšem položaju.

Poleg tega bo Komisija podpirala razvoj varnostnih standardov in pomagala pri prostovoljnih evropskih shemah certificiranja na področju računalništva v oblaku, pri čemer bo upoštevala potrebo po varnosti podatkov. Osredotočiti bi se bilo treba na varnost dobavne verige, zlasti v ključnih gospodarskih sektorjih (industrijski kontrolni sistemi, energetska in prometna infrastruktura). Ta prizadevanja bi morala temeljiti na tekočem delu evropskih organizacij za standardizacijo (CEN, CENELEC in ETSI)[28] in koordinacijske skupine za kibernetsko varnost (CSCG) ter na strokovnem znanju ENISA, Komisije in drugih ustreznih akterjev.

Komisija bo:

- leta 2013 vzpostavila javno-zasebno **platformo za rešitve na področju VOI**, s katero bo razvijala spodbude za sprejetje rešitev za varno IKT in vzpostavitev učinkovite kibernetske varnosti, ki bi veljala za izdelke IKT v Evropi;
- leta 2014 predlagala priporočila za zagotavljanje kibernetske varnosti po vsej vrednostni verigi IKT, ki bodo temeljila na delu te platforme;
- preučila, kako bi glavni ponudniki strojne in programske opreme IKT nacionalnim pristojnim organom lahko poročali o odkritih ranljivostih, ki bi lahko imele pomembne posledice za varnost.

Komisija poziva ENISA, naj:

- v sodelovanju z ustreznimi nacionalnimi pristojnimi organi, zainteresiranimi stranmi, mednarodnimi in evropskimi organi za standardizacijo in Skupnim raziskovalnim središčem Evropske komisije razvije **tehnične smernice in priporočila za sprejetje standardov in dobrih praks na področju VOI** v javnem in zasebnem sektorju.

Komisija poziva javne in zasebne zainteresirane strani, naj:

- proizvajalce izdelkov IKT in ponudnike storitev, vključno s ponudniki storitev računalništva v oblaku, spodbujajo, da razvijejo in sprejmejo **varnostne standarde**, tehnične predpise in načela vgrajene varnosti ter vgrajene zasebnosti pod vodstvom industrije; nove generacije programske in strojne opreme bi morale biti opremljene z **močnejšimi, vgrajenimi in uporabniku prijaznimi**

[28] Zlasti v okviru standarda za pametna omrežja M/490 za prvi sklop standardov za pametna omrežja in referenčne arhitekture.

varnostnimi elementi;

- pod vodstvom industrije razvijejo standarde za izpolnjevanje zahtev na področju kibernetske varnosti za podjetja in izboljšajo javni dostop do informacij z uvedbo **varnostnih oznak** ali oznak kakovosti, ki bodo potrošnikom omogočale boljši pregled nad trgom.

Spodbujanje naložb v raziskave in razvoj ter inovacij

Raziskave in razvoj lahko podpirajo trdno industrijsko politiko, spodbujajo zanesljivo evropsko industrijo IKT, krepijo notranji trg in zmanjšujejo odvisnost Evrope od tujih tehnologij. Z raziskavami in razvojem bi bilo treba zapolniti vrzeli v varnosti IKT, se pripraviti na naslednjo generacijo varnostnih izzivov, upoštevati stalni razvoj potreb uporabnikov in izkoristiti prednosti tehnologij z dvojno rabo. tako bi morali še naprej podpirati razvoj kriptografije. Ob tem bi si bilo z zagotavljanjem potrebnih spodbud in vzpostavitvijo ustreznih pogojev politike treba prizadevati za prenos rezultatov raziskav in razvoja v komercialne rešitve.

EU bi morala izkoristiti okvirni program za raziskave in inovacije Obzorje 2020[29], ki bo začel delovati leta 2014. Predlog Komisije vsebuje konkretne cilje za zanesljivo IKT in boj proti kibernetski kriminaliteti, ki so v skladu s to strategijo. Program Obzorje 2020 bo spodbujal raziskave na področju varnosti, povezane z nastajajočimi tehnologijami IKT, rešitve za povsem varne sisteme, storitve in aplikacije IKT, pripravljal spodbude za izvedbo in sprejetje obstoječih rešitev in obravnaval interoperabilnost med omrežji in informacijskimi sistemi. Posebna pozornost bo na ravni EU namenjena optimizaciji in boljšemu usklajevanju različnih programov financiranja (Obzorje 2020, Sklad za notranjo varnost, Evropska obrambna agencija, vključno z evropskim okvirom za sodelovanje).

Komisija bo:

- uporabila program Obzorje 2020 za obravnavanje številnih področij zasebnosti in varnosti IKT, od raziskav in razvoja do inovacij in uporabe. V okviru programa Obzorje 2020 se bodo razvijala tudi orodja in instrumenti za boj proti kriminalnim in terorističnim dejavnostim, usmerjenim v kibernetsko okolje;
- vzpostavila mehanizme za boljše usklajevanje raziskovalnih programov institucij Evropske unije in držav članic ter spodbujala države članice, naj več vlagajo v raziskave in razvoj.

Komisija poziva države članice, naj:

- do konca leta 2013 razvijejo dobre prakse za **izkoriščanje kupne moči javnih uprav** (na primer prek javnih naročil), da se bosta pospešila razvoj in uvajanje varnostnih elementov v izdelkih in storitvah IKT;
- spodbujajo zgodnje vključevanje industrije in akademskega sveta v razvoj in usklajevanje rešitev. Pri tem bi bilo treba kar najbolj izkoristiti industrijsko bazo v

[29] Obzorje 2020 je finančni instrument, s katerim se bo izvajala Unija inovacij, vodilna pobuda iz strategije Evropa 2020, katere cilj je zagotoviti konkurenčnost Evrope v svetu. Od leta 2014 do leta 2020 bo ta novi okvirni program EU za raziskave in inovacije del prizadevanj za novo rast in delovna mesta v Evropi.

Evropi in povezane tehnološke inovacije, dosežene z raziskavami in razvojem, pri čemer bi bilo treba uskladiti raziskovalne programe civilnih in vojaških organizacij.

Komisija poziva Europol in ENISA, naj:

- opredelita nove trende in potrebe v povezavi z razvijajočimi se vzorci kibernetske kriminalitete in varnosti, da bosta lahko razvila ustrezna digitalna orodja in tehnologije.

Komisija poziva javne in zasebne zainteresirane strani, naj:

- v sodelovanju z zavarovalniškim sektorjem razvijejo **usklajena merila za izračun premij za tveganje**, da bi podjetja, ki so vlagala v varnost, lahko plačala nižje prispevke za zavarovanje.

2.5. Oblikovanje usklajene mednarodne kibernetske politike Evropske unije in spodbujanje temeljnih vrednot EU

Ohranjanje odprtega, svobodnega in varnega kibernetskega prostora je svetovni izziv, ki bi ga morala EU obravnavati skupaj z ustreznimi mednarodnimi partnerji in organizacijami, zasebnim sektorjem in civilno družbo.

V okviru mednarodne kibernetske politike si bo EU prizadevala za odprt in svoboden internet, spodbujala opredelitev pravil vedenja in v kibernetskem prostoru uporabila obstoječe mednarodne zakone. Prav tako si bo prizadevala za zmanjšanje digitalne ločnice in dejavno sodelovala pri mednarodnih prizadevanjih za gradnjo zmogljivosti na področju kibernetske varnosti. Mednarodna vključenost EU v obravnavanje kibernetskih vprašanj bo temeljila na osrednjih vrednotah človekovega dostojanstva, svobode, demokracije, enakopravnosti, pravne države in spoštovanja temeljnih pravic.

Vključevanje kibernetskih vprašanj v zunanje odnose EU in skupno zunanjo in varnostno politiko

Komisija, visoka predstavnica in države članice bi morale oblikovati usklajeno mednarodno kibernetsko politiko EU, katere cilj bo večja vključenost in okrepljeni odnosi s ključnimi mednarodnimi partnerji in organizacijami ter s civilno družbo in zasebnim sektorjem. Posvetovanja EU z mednarodnimi partnerji o kibernetskih vprašanjih bi morala biti zasnovana, usklajena in izvedena tako, da bi dopolnila obstoječe dvostranske dialoge med državami članicami EU in tretjimi državami. EU se bo ponovno posvetila dialogu s tretjimi državami, zlasti s podobno mislečimi partnerji, ki imajo podobne vrednote kot EU. Spodbujala bo visoko raven varstva podatkov, tudi pri prenosu osebnih podatkov v tretje države. Pri reševanju svetovnih kibernetskih izzivov si bo EU prizadevala za tesnejše sodelovanje med organizacijami, dejavnimi na tem področju, kot so Svet Evrope, OECD, ZN, OVSE, NATO, AU, ASEAN in OAS. Na dvostranski ravni je še posebej pomembno sodelovanje z Združenimi državami, ki se bo še naprej razvijalo, zlasti v okviru delovne skupine EU–ZDA za kibernetsko varnost in kibernetsko kriminaliteto.

Eden glavnih elementov mednarodne kibernetske politike EU bo ohranjanje kibernetskega prostora kot območja svobode in temeljnih pravic. Z razširitvijo dostopa do interneta bi morale demokratične reforme po vsem svetu dobiti podporo in spodbudo. Povečane povezanosti na svetovni ravni pa ne bi smela spremljati cenzura ali množični nadzor. EU bi

morala spodbujati družbeno odgovornost gospodarskih družb[30] in sprožiti mednarodne pobude za izboljšanje svetovnega usklajevanja na tem področju.

Odgovornost za varnejši kibernetski prostor nosijo vsi akterji svetovne informacijske družbe, od državljanov do vlad. EU podpira prizadevanja za opredelitev pravil vedenja v kibernetskem prostoru, ki bi se jih morale držati vse zainteresirane strani. Od državljanov pričakuje, da bodo spoštovali svoje državljanske dolžnosti, socialne odgovornosti in zakone tudi na spletu, prav tako pa bi se predpisov in obstoječih zakonov morale držati države. Na področju mednarodne varnosti EU spodbuja oblikovanje ukrepov za krepitev zaupanja v kibernetsko varnost, da bi se povečala preglednost in zmanjšalo tveganje napačnega razumevanja ravnanja držav.

EU ne poziva k oblikovanju novih mednarodnih pravnih instrumentov za obravnavo kibernetskih vprašanj.

Pravne obveznosti iz Mednarodnega pakta o političnih in državljanskih pravicah, Evropske konvencije o človekovih pravicah in Listine Evropske unije o temeljnih pravicah bi morale veljati tudi na spletu. EU se bo osredotočila na vprašanje, kako zagotoviti, da bodo se bodo ti instrumenti izvajali tudi v kibernetskem prostoru.

Konvencija iz Budimpešte je instrument za obravnavo kibernetske kriminalitete, ki ga lahko sprejmejo tudi tretje države. Služi lahko kot model za pripravo nacionalne zakonodaje na področju kibernetske kriminalitete in kot podlaga za mednarodno sodelovanje na tem področju.

Če se bodo oboroženi spopadi razširili na kibernetski prostor, se bo v zadevnem primeru upoštevalo mednarodno humanitarno pravo in po potrebi pravo o človekovih pravicah.
Gradnja zmogljivosti za kibernetsko varnost in vzpostavitev odpornih informacijskih infrastruktur v tretjih državah

S tesnejšim mednarodnim sodelovanjem se bo izboljšalo nemoteno delovanje ključnih infrastruktur, ki zagotavljajo in omogočajo komunikacijske storitve. To sodelovanje vključuje izmenjavo najboljše prakse in informacij, zgodnje opozarjanje, skupne vaje na področju obvladovanja incidentov itd. EU bo k temu cilju prispevala tako, da bo okrepila tekoča mednarodna prizadevanja za izboljšanje mrež za sodelovanje za zaščito kritične informacijske infrastrukture, v katerih so dejavni vlade in zasebni sektor.

Prednosti interneta še ne morejo izkoristiti v vseh delih sveta, saj ponekod nimajo odprtega, varnega, interoperabilnega in zanesljivega dostopa. EU bo zato še naprej podpirala prizadevanja držav, da svojim državljanom omogočijo dostop in uporabo interneta, zagotovijo njegovo celovitost in varnost ter se učinkovito borijo proti kibernetski kriminaliteti.

V sodelovanju z državami članicami bosta Komisija in visoka predstavnica:

- delovali v smeri usklajene mednarodne kibernetske politike EU, da se poveča vključenost ključnih mednarodnih partnerjev in organizacij, vključi kibernetska vprašanja v SZVP ter izboljša usklajevanje na področju globalnih kibernetskih vprašanj;

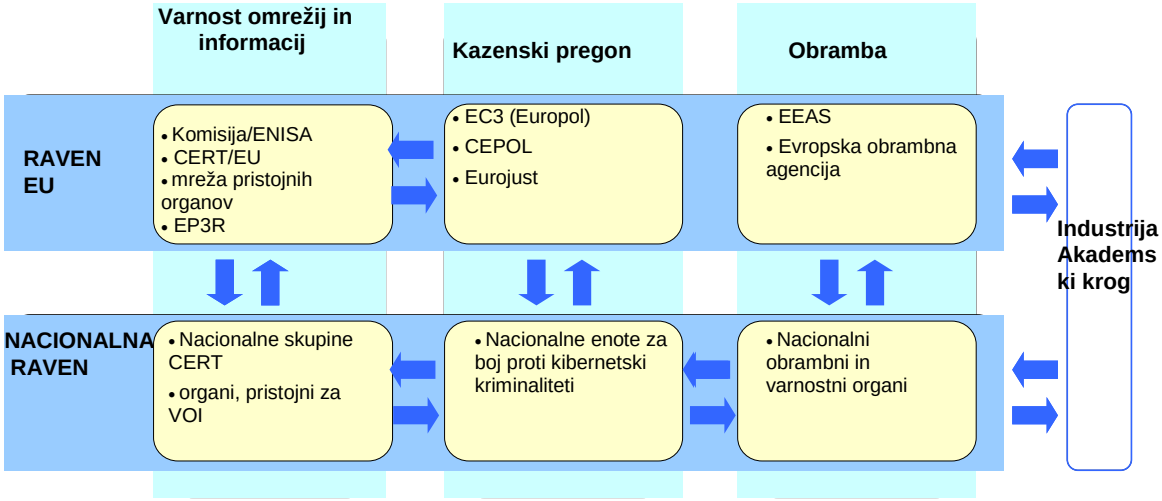
[30] Obnovljena strategija EU za družbeno odgovornost podjetij za obdobje 2011–2014, COM(2011) 681 final.

- podpirali opredelitev pravil vedenja in ukrepov za krepitev zaupanja v kibernetsko varnost, omogočali dialog o tem, kako uporabiti obstoječe mednarodno pravo v kibernetskem prostoru, in spodbujali uporabo konvencije iz Budimpešte za obravnavo kibernetske kriminalitete;
- podpirali spodbujanje in varstvo temeljnih pravic, vključno z dostopom do informacij in svobodo izražanja, ter se pri tem osredotočili na: a) oblikovanje novih javnih smernic za svobodo izražanja v spletnem in nespletnem okolju; b) spremljanje izvoza izdelkov ali storitev, ki bi se lahko uporabili za cenzuro ali množični nadzor na spletu; c) oblikovanje ukrepov in orodij za povečanje dostopnosti, odprtosti in odpornosti interneta za boj proti cenzuri ali množičnemu nadzoru s komunikacijsko tehnologijo; d) omogočanje zainteresiranim stranem, da uporabijo komunikacijske tehnologije za spodbujanje temeljnih pravic;
- v sodelovanju z mednarodnimi partnerji in organizacijami, zasebnim sektorjem in civilno družbo podpirali gradnjo zmogljivosti v tretjih državah po vsem svetu, s čimer bi izboljšali dostop do informacij in odprtega interneta, preprečili in odpravili kibernetske grožnje (tudi naključne), kibernetsko kriminaliteto in kibernetski terorizem ter razvili usklajevanje med donatorji, da bi bili ukrepi za gradnjo zmogljivosti ciljno usmerjeni;
- uporabljali različne instrumente EU za gradnjo zmogljivosti na področju kibernetske varnosti, na primer z usposabljanjem osebja organov za kazenski pregon in pravosodje ter tehničnega osebja za obravnavanje kibernetskih groženj, pa tudi s podporo za oblikovanje ustreznih nacionalnih politik, strategij in ustanov v tretjih državah;
- povečali usklajevanje politik in izmenjavo informacij prek mednarodnih mrež za zaščito kritične informacijske infrastrukture (npr. Meridian) in v sodelovanju z organi, pristojnimi za VOI, ter drugimi akterji.

3. VLOGE IN ODGOVORNOSTI

Kibernetski incidenti v prepletenem digitalnem gospodarstvu in družbi ne poznajo meja. Vsi akterji, od organov, pristojnih za VOI, CERT in organov pregona do industrije, morajo prevzeti odgovornost tako na nacionalni ravni kot na ravni EU in sodelovati, da bi okrepili kibernetsko varnost. Ker so lahko vključeni različni pravni okviri in pristojnosti, je glavni izziv za EU, da pojasni vloge in odgovornosti številnih vključenih akterjev.

Glede na zapletenost vprašanja in raznovrstnost vključenih akterjev centraliziran evropski nadzor ni rešitev. Nacionalne vlade so v najboljšem položaju, da organizirajo preprečevanje in odzivanje na kibernetske incidente in napade ter s svojimi politikami in pravnimi okviri vzpostavijo stike in mreže z zasebnim sektorjem in splošno javnostjo. Hkrati pa bi bilo zaradi možne ali dejanske čezmejne narave tveganj za učinkovit nacionalni odziv pogosto potrebno sodelovanje na ravni EU. Za celovito obravnavanje kibernetske varnosti bi morale dejavnosti vključevati tri ključna področja: VOI, kazenski pregon in obrambo, za katera se uporabljajo različni pravni okviri:



3.1. Usklajevanje med organi, pristojnimi za VOI/skupinami CERT ter organi za kazenski pregon in obrambo

Nacionalna raven

Države članice bi morale že imeti vzpostavljene strukture za obravnavanje kibernetske odpornosti, kibernetske kriminalitete in obrambe ali pa te strukture vzpostaviti na podlagi te strategije; prav tako bi morale doseči zahtevano raven zmogljivosti za obravnavanje kibernetskih incidentov. Glede na veliko število organov, ki so operativno odgovorni za različna področja kibernetske varnosti, in glede na pomembnost vključevanja zasebnega sektorja bi bilo treba na nacionalni ravni zagotoviti optimalno usklajevanje med ministrstvi. Države članice bi morale v svojih nacionalnih strategijah za kibernetsko varnost določiti vloge in odgovornosti različnih nacionalnih organov.

Treba bi bilo spodbujati izmenjavo informacij med nacionalnimi organi in zasebnim sektorjem, da bi obe strani ohranili celovit pregled nad različnimi nevarnostmi ter pridobili boljše razumevanje novih trendov in tehnik, ki se lahko uporabljajo tako za izvajanje kibernetskih napadov kot za hitrejše odzivanje nanje. Z nacionalni načrti sodelovanja na področju VOI, ki bi se uporabljali v primeru kibernetskih incidentov, bi morale države članice jasno dodeliti vloge in odgovornosti ter izboljšati odziv.

Raven EU

Tako kot na nacionalni ravni se tudi na ravni EU s kibernetsko varnostjo ukvarja več akterjev. ENISA, Europol/EC3 in EDA so tri agencije, zlasti dejavne na področju VOI, kazenskega pregona in obrambe. Države članice so zastopane v upravnih odborih teh agencij, ki zagotavljajo platforme za usklajevanje na ravni EU.

Usklajevanje in sodelovanje med ENISA, Europolom/EC3 in EDA se bo spodbujalo na več področjih, na katerih so te agencije skupaj dejavne, zlasti pri analizi trendov, oceni tveganja, usposabljanju in izmenjavi najboljših praks. Ob sodelovanju pa bi morale agencije ohraniti svoje posebnosti. Skupaj s CERT-EU, Komisijo in državami članicami bi morale podpreti razvoj zanesljive skupnosti tehničnih in političnih strokovnjakov na tem področju.

Neformalne kanale za usklajevanje in sodelovanje bo dopolnjevalo več strukturnih povezav. V okviru vojaškega štaba EU in projektne skupine EDA za kibernetsko obrambo bi lahko

potekalo usklajevanje na področju obrambe. Programski odbor Europola/EC3 bo med drugim združeval EUROJUST, CEPOL, države članice[31], ENISA in Komisijo ter zagotovil izmenjavo njihovih različnih strokovnih znanj in partnersko izvajanje ukrepov EC3 ob upoštevanju strokovnega znanja in pooblastil vseh zainteresiranih strani. Novi mandat ENISA bi moral omogočiti boljšo povezavo z Europolom in zainteresiranimi stranmi iz industrije. Najpomembnejše pa je, da bi se z zakonodajnim predlogom Komisije o VOI vzpostavil okvir za sodelovanje prek mreže nacionalnih organov, pristojnih za VOI, ter uredila izmenjava informacij med organi za VOI in organi kazenskega pregona.

Mednarodna raven

Komisija in visoka predstavnica skupaj z državami članicami zagotavljata usklajeno mednarodno ukrepanje na področju kibernetske varnosti. Pri tem bosta Komisija in visoka predstavnica podpirali ključne vrednote in spodbujali mirno, odprto in pregledno uporabo kibernetskih tehnologij. Komisija, visoka predstavnica in države članice se vključujejo v politični dialog z mednarodnimi partnerji in mednarodnimi organizacijami, kot so Svet Evrope, OVSE, NATO in Združeni narodi.

3.2. Podpora EU v primeru večjih kibernetskih incidentov ali napadov

Večji kibernetski incidenti ali napadi lahko vplivajo na vlade, podjetja in posameznike v EU. Ta strategija in zlasti predlog direktive o VOI bi morala izboljšati preprečevanje, odkrivanje in odzivanje na kibernetske incidente ter povečati obseg obveščanja o večjih kibernetskih incidentih ali napadih med državami članicami in Komisijo. Vendar se bodo mehanizmi za odzivanje razlikovali glede na naravo, obseg in čezmejne posledice incidenta.

Če incident resno vplivala na neprekinjeno poslovanje, direktiva o VOI predlaga, da se uporabijo nacionalni načrti ali načrti Unije za sodelovanje na področju VOI, odvisno od čezmejne narave incidenta. Mreža organov, pristojnih za VOI, bi se v takem primeru uporabila za izmenjavo informacij in podporo. To bi omogočilo ohranjanje in/ali obnovo prizadetih omrežij in storitev.

Če se zdi, da je incident povezan s kaznivim dejanjem, bi bilo treba obvestiti Europol/EC3, da lahko skupaj z organi pregona iz prizadetih držav začne preiskavo, ohrani dokaze, identificira storilce in zagotovi njihov pregon.

Če se zdi, da je incident povezan s kibernetskim vohunjenjem ali državno vodenim napadom, ali pa ima posledice za nacionalno varnost, bodo nacionalni organi za varnost in obrambo o tem obvestili ustrezne partnerje, da bodo ti vedeli, da so napadeni in da se bodo lahko branili. Aktivirani bodo mehanizmi zgodnjega opozarjanja in po potrebi postopki za krizno upravljanje ali drugi postopki. Posebej resni kibernetski incidenti ali napadi so lahko zadosten razlog, da država članica uveljavlja solidarnostno klavzulo EU (člen 222 Pogodbe o delovanju Evropske unije).

Če se zdi, da je incident ogrozil varstvo osebnih podatkov, bi morali biti v skladu z Direktivo 2002/58/ES o tem obveščeni nacionalni organi za varstvo podatkov ali nacionalni regulativni organi.

[31] Prek predstavništva v okviru projektne skupine EU za boj proti kibernetski kriminaliteti, ki jo sestavljajo vodje enot za boj proti kibernetski kriminaliteti v državah članicah.

Poleg tega se bo pri obravnavanje kibernetskih incidentov in napadov mogoče opreti na kontaktne mreže in podporo mednarodnih partnerjev. Ta lahko vključuje tehnične ukrepe za ublažitev škode, kazenske preiskave ali aktiviranje mehanizmov za krizno upravljanje in odzivanje.

4. ZAKLJUČEK IN NADALJNJI UKREPI

Ta strategija za kibernetsko varnost EU, ki jo predlagata Komisija in visoka predstavnica Unije za zunanje zadeve in varnostno politiko, predstavlja vizijo EU in potrebne ukrepe, da bo ob močni zaščiti in spodbudi pravic državljanov spletno okolje EU postalo najvarnejše na svetu[32].

To vizijo je mogoče uresničiti samo z resničnim partnerstvom med številnimi akterji, ki morajo prevzeti odgovornost in se soočiti s prihodnjimi izzivi.

Komisija in visoka predstavnica zato pozivata Evropski svet in Evropski parlament, da strategijo podpreta in pomagata izvesti navedene ukrepe. Potrebna je tudi močna podpora in vključenost zasebnega sektorja in civilne družbe, ki sta ključna akterja za izboljšanje varnosti in zaščito pravic državljanov.

Ukrepati je treba takoj. Komisija in visoka predstavnica sta odločeni, da si bosta skupaj z vsemi akterji prizadevali, da bi v Evropi zagotovili potrebno varnost. Da se zagotovi hitro izvajanje strategije in njeno pregledovanje v skladu z morebitnim novim razvojem, bodo vse zadevne strani čez 12 mesecev povabljene na konferenco na visoki ravni, kjer bo ocenjen napredek.

[32] Strategija bo financirana v okviru predvidenih zneskov za posamezna ustrezna področja politike (IPE, Obzorje 2020, Sklad za notranjo varnost, SZVP in zunanje sodelovanje, zlasti instrument za stabilnost), kot je določeno v predlogu Komisije za večletni finančni okvir za obdobje 2014–2020 (glede na odobritev proračunskega organa in končne zneske sprejetega večletnega finančnega okvira za obdobje 2014–2020). Da se ne bi prekoračilo skupno število delovnih mest, ki so na voljo decentraliziranim agencijam in da bi se upoštevale zgornje meje za te agencije v vsakem razdelku odhodkov v naslednjem večletnem finančnem okviru, se bo agencije, ki jim to sporočilo nalaga nove naloge (CEPOL, EDA ENISA, EUROJUST in EUROPOL/EC3), spodbujalo, da pred začetkom opravljanja teh nalog preverijo dejanske zmogljivosti agencije za pokritje novih virov in preučijo vse možnosti za prerazporeditev.