Eiropas Savienības
Padome

Briselē, 2017. gada 11. aprīlī
(OR. en)

5387/1/17
REV 1 DCL 1

GENVAL 4
CYBER 11

DEKLASIFIKĀCIJA

Dokuments:	5387/1/17 REV 1 RESTREINT UE
Datums:	2017. gada 1. marts
Jauns statuss:	Publiski pieejams
Temats:	Novērtējuma ziņojums par savstarpējo izvērtējumu septīto kārtu "Eiropas kibernoziedzības novēršanas un apkarošanas politikas praktiskā īstenošana un darbība" – ziņojums par Latviju

Pielikumā pievienota iepriekš minētā dokumenta deklasificēta versija.

Šā dokumenta teksts ir ident iepriekšējai versijai.

Eiropas Savienības
Padome

Briselē, 2017. gada 1. martā
(OR. en)

5387/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 4
CYBER 11

ZIŅOJUMS

Temats:	Novērtējuma ziņojums par savstarpējo izvērtējumu septīto kārtu "Eiropas kibernoziedzības novēršanas un apkarošanas politikas praktiskā īstenošana un darbība" – ziņojums par Latviju

PIELIKUMS

Saturs

1. KOPSAVILKUMS

Latvijas iestādes apmeklējumu bija sagatavojušas ļoti labi, un tas ietvēra tikšanās ar attiecīgajām struktūrām, kas iesaistītas kibernoziedzības novēršanā un apkarošanā un ES politikas īstenošanā un darbībā (piemēram, ar Iekšlietu ministriju, Aizsardzības ministriju, Drošības policiju, Valsts policiju, Tieslietu ministriju un Ģenerālprokuratūru). Apmeklējums bija sagatavots un tika koordinēts lieliski. Latvijas Iekšlietu ministrija, kas koordinēja apmeklējumu un dažādas tikšanās ar ieinteresētajām personām, bija ļoti izpalīdzīga un bija gatava organizēt papildu tikšanās ar ekspertiem ikreiz, kad izvērtēšanas grupai bija neskaidri jautājumi. Notika arī tikšanās ar privātām organizācijām, kurām ir nozīmīga loma kibernoziedzības apkarošanā un novēršanā un kiberdrošības uzlabošanā (CERT.LV, Digitālās drošības alianse, *Net-Safe Latvia* un Latvijas Informācijas un komunikācijas tehnoloģijas asociācija (LIKTA)), un tas deva labu pārskatu par to, kā darbojas publiskā-privātā partnerība.

Latvija ir pieņēmusi Latvijas Kiberdrošības stratēģiju 2014–2018 un rīcības plānu tās īstenošanai. Stratēģijā ir paredzēta virkne soļu, kas tiek veikti ar mērķi uzlabot Latvijas esošās rīcībspējas kibernoziedzības apkarošanā. Stratēģija aptver piecas prioritārās jomas, tādas kā: 1) kiberdrošības pārvaldība un resursi; 2) tiesiskums kibertelpā un kibernoziedzības mazināšana; 3) gatavība un rīcībspēja krīzes situācijās; 4) sabiedrības izpratne, izglītība un pētniecība; 5) starptautiskā sadarbība. Otrā galvenā joma ir vērsta uz leģislatīvu grozījumu pieņemšanu, cita starpā nosakot krimināltbildību par uzbrukumiem automatizētām datu apstrādes sistēmām; uz spēju veidošanas un mācību pasākumiem; pasākumiem kibernoziedzības novēršanai un apkarošanai; sabiedrības informēšanas pasākumiem; kā arī starptautiskās sadarbības pasākumiem.

IT drošības un aizsardzības politikas veidošanu un īstenošanu koordinē Aizsardzības ministrija, kas ir atbildīga arī par starptautisko sadarbību. Taču par kibernoziedzības apkarošanu atbild tikai Iekšlietu ministrija – galvenokārt Valsts policija un konkrētos gadījumos Drošības policija. Valsts policijas atbildībā ir apkarot nodarījumus pret datorizētu datu un datorsistēmu konfidencialitāti, neaizskaramību un pieejamību (nelikumīga piekļuve, nelikumīga pārtveršana, iejaukšanās datos, iejaukšanās sistēmās, ļaunprātīga ierīču izmantošana); ar datoriem saistītus nodarījumus (ar datoriem saistīta viltošana, datorkrāpšana); ar saturu saistītus nodarījumus (ar bērnu pornogrāfiju saistīti pārkāpumi); un ar autortiesību un blakustiesību pārkāpšanu saistītus nodarījumus. Valsts policijas un Drošības policijas atbildībā ir apkarot rasistisku un ksenofobisku materiālu izplatīšanu datorsistēmās.

Koordinācijas pamatā ir savstarpējas sadarbības princips, katrai iestādei vai struktūrai veicot savas funkcijas un – vai nu tieši, vai caur Nacionālo IT drošības padomi (Padomi) – sadarbojoties ar pārējiem iesaistītajiem. Padome ir arī centrālā platforma informācijas apmaiņai un sadarbībai starp publisko sektoru un privātā sektora struktūrām, tādām kā finanšu iestādes un NVO. Plašais dalībnieku loks, šķiet, palīdz nodrošināt labu sadarbību un informācijas plūsmu starp visām attiecīgajām ieinteresētajām personām.

Kopumā jāatzīmē, ka Latvija patiesi cenšas pēc iespējas labāk izmantot ierobežotos pieejamos resursus kibernoziedzības apkarošanai. Uzslavējama ir Kiberdrošības stratēģijā izvirzītā ideja vienkāršot dažādo Valsts policijas struktūrvienību struktūru un ierobežot to funkciju sadalījumu, lai panāktu vislabāko iespējamo ieguldījumu atdevi. Viens no risinājumiem varētu būt atbildību par kibernoziedzību koncentrēt vienā Valsts policijas struktūrvienībā, kas saņemtu konkrētu atbalstu no Infotehnisko ekspertīžu nodaļas. Bez tam būtu arī turpmāk jācenšas uzturēt un palielināt resursus valsts kibernoziedzības apkarošanas spēju stiprināšanai, īpaši Valsts policijas līmenī.

Šķiet, ka pastāv aktīva sadarbība starp Valsts policiju un nevalstiskajām organizācijām, tādām kā *Net-Safe*, kā arī starp Valsts policiju un CERT.LV. Jo īpaši *Net-Safe* bieži sadarbojas ar Valsts policiju, ja rodas nopietnas aizdomas par nepilngadīgo seksuālu izmantošanu.

Net-Safe uzdevums ir novērst kibernoziedzību un sniegt atbalstu gadījumos, kas saistīti ar bērnu seksuālu izmantošanu tiešsaistē un pornogrāfiju. CERT.LV ir nozīmīga loma reakcijā uz kiberincidentiem, un tā darbojas kā starpnieks starp privāto sektoru, akadēmisko sektoru un policiju. Tā ir prasmīgs un sadarboties gatavs partneris publiskajām iestādēm un sabiedrībai kopumā (piemēram, tā piedāvā ierīču informācijas dzēšanas pakalpojumus).

Kas attiecas uz likumdošanu, Latvija ir parakstījusi un ratificējusi Konvenciju par kibernoziegumiem un savos tiesību aktos īstenojusi ar kibernoziedzību saistītās ES direktīvas. Tāpat kā daudzās citās valstīs Latvijas tiesību aktos nav dota konkrēta kibernoziedzības definīcija. Praksē kibernoziedzība ietver visus nodarījumus pret datorsistēmām un datorizētiem datiem, kā arī nodarījumus, kas veikti, izmantojot datorsistēmu.

Latvija arī strādā pie tā, lai ieviestu labāku prevencijas stratēģiju, kuras mērķis ir uzlabot informētību par iespējamiem draudiem, ko var radīt darbības tiešsaistē. Lielāka skaita attiecīgo neaizsargāto grupu mērķtiecīga informēšana vēl vairāk palīdzētu uzlabot Latvijas kibervides vispārējo drošību. Dažādas publiskas struktūras Latvijā ir ieviesušas daudzus preventīvus pasākumus, tomēr tie ne vienmēr ir koordinēti. Izvērtētāji uzskata, ka visai valstij par labu nāktu vienota kontaktpunkta izmantošana preventīvu darbību koordinēšanai starp ministrijām un citām attiecīgām organizācijām, jo tas novērstu preventīvā darba dublēšanos.

Latvijas iestādes pazīst un izmanto ES aģentūras. Tā kā lielāko daļu izmeklēšanu veic Valsts policija, tieši tā līdz šim ir piedalījusies *Eurojust* koordinācijas sanāksmēs un, visticamāk, turpinās to darīt arī nākotnē. Tāpēc Valsts policija arī lielākajā daļā gadījumu atbild par starpvalstu sadarbību kibernoziegumu lietu izmeklēšanā, izmantojot Eiropola/*EC3* sistēmu. Tomēr Latvijas iestādes uzskata, ka ir vajadzīgi risinājumi ES līmenī, kā uzlabot un paātrināt savstarpējās tiesiskās palīdzības izpildi, tiesu iestāžu sadarbību un saziņu starp dalībvalstīm un trešām valstīm, kā arī tiešu sadarbību ar ārvalstu interneta pakalpojumu sniedzējiem.

Latvijas Tiesnešu mācību centrs organizē mācības tiesnešiem, un vajadzības gadījumā var tikt rīkotas arī mācības par kibernoziedzību. Arī prokurori tiek apmācīti – bet abos gadījumos mācības nav obligātas un tajās piedalās tikai ierobežots praktiķu skaits. Latvijas spējas cīnīties pret kibernoziedzību varētu būt labākas, ja būtu šajā jomā specializēti prokurori. Policisti gan ir labi apmācīti. Valsts policijas koledža piedāvā policistiem visaptverošu kibernoziedzības mācību programmu ar dažādiem moduļiem. Kopīgi mācību kursi, kuros iesaistītos Valsts policija un tiesu iestādes, varētu palīdzēt vairot zināšanas par kibernoziedzību un darboties kā platforma pieredzes apmaiņai, ietverot tādas tēmas kā policijai pieejamās iespējas un tehniskie paņēmieni vai arī tiesnešiem un prokuroriem nozīmīgie jautājumi ar kibernoziedzību saistītos kriminālprocesos.

Izmantojot ierobežotus resursus, Latvija cenšas paveikt maksimālo kopīgajā cīņā pret kibernoziedzību, pēc iespējas vairāk integrējot ārpus valsts pārvaldes pieejamos resursus. Uzskatāms piemērs ir Zemessardzes Kiberaizsardzības vienības izveidošana – šī vienība, ko veido Latvijas privātā sektora eksperti, darbosies kā spēju rezerve kiberkrīzes gadījumā. Vēl viens piemērs ir jauniešu un citu brīvprātīgo iesaiste, piemēram, informēšanas pasākumos. Papildus tam ir pierādījies, ka ļoti efektīva metode, kā reāli sasniegt mērķauditoriju, ir vienaudžu vadīti pasākumi (jaunieši uzrunā citus jauniešus viņu pašu valodā) prevencijas un informēšanas kampaņās. Trešais piemērs ir labā sadarbība ar kiberjomas NVO, piemēram, Latvijas Drošāka interneta centru. Lai turpinātu šo labo sadarbību, būtu jāapsver iespējas sniegt NVO pietiekamu atgriezenisko informāciju par sadarbības rezultātiem.

Latvijas stratēģija ir acīmredzami padarīt valsti nepievilcīgu kibernoziedzniekiem un sagatavoties iespējamai krīzei. Izvērtējot pastāvošās struktūras, valsts ieguldītās pūles cīņā pret kibernoziedzību un šo ieguldījumu efektivitāti, izvērtētāju viedoklis ir nepārprotami pozitīvs.

2. IEVADS

Pēc Vienotās rīcības 97/827/TI (1997. gada 5. decembris) [1] pieņemšanas tika izveidots mehānisms, lai izvērtētu, kā valsts līmenī tiek piemēroti un īstenoti starptautiski pasākumi cīņā pret organizēto noziedzību. Saskaņā ar Vienotās rīcības 2. pantu Vispārējo jautājumu, tostarp izvērtējumu, darba grupa (*GENVAL*) 2013. gada 3. oktobrī nolēma, ka septītajā savstarpējo izvērtējumu kārtā vajadzētu vērtēt to, kā praktiski tiek īstenota un kā darbojas ES kibernoziedzības novēršanas un apkarošanas politika.

Kibernoziedzības izvēli par septītās savstarpējo izvērtējumu kārtas tematu dalībvalstis novērtēja atzinīgi. Tomēr, tā kā kibernoziedzības jēdziens ietver plašu nodarījumu loku, tika panākta vienošanās, ka izvērtējumā galvenais uzsvars būs uz tiem nodarījumiem, kuri dalībvalstu ieskatā pelna īpašu uzmanību. Tāpēc izvērtējumā ir iekļautas trīs konkrētas jomas: kiberuzbrukumi, bērnu seksuālā izmantošana un pornogrāfija tiešsaistē, krāpnieciski darījumi ar norēķinu kartēm tiešsaistē. Izvērtējumā būtu visaptveroši jāizskata kibernoziedzības apkarošanas juridiskie un operatīvie aspekti, pārrobežu sadarbība un sadarbība ar attiecīgajām ES aģentūrām. Šajā kontekstā īpaši nozīmīga ir Direktīva 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu [2] (transponēšanas datums – 2013. gada 18. decembris) un Direktīva 2013/40/ES [3] par uzbrukumiem informācijas sistēmām (transponēšanas datums – 2015. gada 4. septembris).

1 Vienotā Rīcība (1997. gada 5. decembris) (97/827/TI), OV L 344, 15.12.1997., 7. lpp.
2 OV L 335, 17.12.2011., 1. lpp.
3 OV L 218, 14.8.2013., 8. lpp.

Turklāt Padomes 2013. gada jūnija secinājumos [4] par ES kiberdrošības stratēģiju ir atkārtoti minēts mērķis pēc iespējas drīz ratificēt Eiropas Padomes 2001. gada 23. novembra Konvenciju par kibernoziegumiem (Budapeštas konvenciju) [5] un secinājumu preambulā uzsvērts, ka "ES neaicina radīt jaunus starptautiskus tiesību instrumentus, kas reglamentētu kiberjautājumus". Konvenciju papildina Protokols par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās [6].

Iepriekšējos izvērtējumos gūtā pieredze liecina, ka dalībvalstu situācija attiecīgo juridisko instrumentu īstenošanā būs atšķirīga, un pašreizējā izvērtēšana varētu arī sniegt noderīgu informāciju tām dalībvalstīm, kuras varbūt vēl nav īstenojušas visus dažādo instrumentu aspektus. Tomēr ir paredzēts, ka izvērtējumam jābūt plašam un starpdisciplināram un tajā jāvērtē ne tikai dažādo ar kibernoziedzības apkarošanu saistīto instrumentu īstenošana, bet arī operatīvie aspekti dalībvalstīs.

Tāpēc papildus sadarbībai ar prokuratūras dienestiem tajā vērtēs arī to, kā policijas iestādes sadarbojas ar *Eurojust*, *ENISA* un Eiropolu/*EC3*, un to, kā šo organizācija dotā atgriezeniskā informācija tiek novadīta līdz attiecīgajiem policijas un sociālajiem dienestiem. Izvērtējumā galvenā uzmanība ir vērsta uz to, kā tiek īstenota valstu politika kiberuzbrukumu, krāpniecības un bērnu pornogrāfijas novēršanai. Tajā vērtēta arī dalībvalstu starptautiskās sadarbības operatīvā prakse un kibernoziedzībā cietušajiem piedāvātais atbalsts.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[5] *CETS* Nr. 185, atvērta parakstīšanai 2001. gada 23. novembrī, stājās spēkā 2004. gada 1. jūlijā.

[6] *CETS* Nr. 189, atvērts parakstīšanai 2003. gada 28. janvārī, stājās spēkā 2006. gada 1. martā.

Dalībvalstu apmeklēšanas secību *GENVAL* pieņēma 2014. gada 1. aprīlī. Latvija bija divdesmitā dalībvalsts, kuru izvērtē šajā kārtā. Saskaņā ar Vienotās rīcības 3. pantu prezidentvalsts paredzētajai izvērtēšanai ir sagatavojusi ekspertu sarakstu. Pēc rakstiska lūguma, ko *GENVAL* priekšsēdētājs 2014. gada 28. janvārī nosūtīja delegācijām, dalībvalstis ir izvirzījušas ekspertus ar pamatīgām praktiskajām zināšanām šajā jomā.

Katra izvērtēšanas grupa sastāv no trim nacionālajiem ekspertiem, kuriem palīdz divi Padomes Ģenerālsekretariāta darbinieki un novērotāji. *GENVAL* piekrita prezidentvalsts ierosinājumam septītajā savstarpējo izvērtējumu kārtā kā novērotājus uzaicināt Eiropas Komisiju, *Eurojust*, *ENISA* un Eiropolu/*EC3*.

Eksperti, kam tika uzticēts Latvijas izvērtējums, ir *Geert Schoorens* kungs (Beļģija), *Søren Palsgaard* kungs (Dānija) un *Marcin Golizda-Bliziński* kungs (Polija). Bija klāt arī divi novērotāji: *Tomas Zbihlej* kungs (*Eurojust*) un *Sławomir Buczma* kungs (Padomes Ģenerālsekretariāts).

Šo ziņojumu sagatavoja ekspertu grupa ar Padomes Ģenerālsekretariāta palīdzību, pamatojoties uz konstatējumiem izvērtēšanas apmeklējumā, kas notika Latvijā no 2016. gada 8. līdz 11. martam, un uz Latvijas detalizētajām atbildēm uz izvērtējuma anketas jautājumiem un papildjautājumiem.

3. VISPĀRĪGI JAUTĀJUMI UN STRUKTŪRAS

3.1. Nacionālā kiberdrošības stratēģija

2014. gada janvārī Ministru kabinets pieņēma Latvijas Kiberdrošības stratēģiju 2014–2018. Kiberdrošības politikas mērķis ir izveidot drošu un uzticamu kibertelpu, kurā ir garantēta valstij un sabiedrībai būtisku pakalpojumu droša, uzticama un nepārtraukta piegāde. Īstenojot kiberdrošības politiku, tiek ievēroti šādi pamatprincipi – attīstība, sadarbība, atbildība un atvērtība.

Viena no piecām galvenajām rīcības jomām ir tiesiskums kibertelpā un kibernoziedzības mazināšana (4.2. sadaļa). Norādīts, ka kibernoziedzības mazināšanai ir nepieciešama rīcība divos pamata virzienos:

– preventīvs darbs noziedzīgu darbību īstenošanas mazināšanai;
– efektīva noziedzības apkarošana.

3.2. Nacionālās prioritātes kibernoziedzības jomā

A. Nacionālās prioritātes

Nacionālās prioritātes kibernoziedzības jomā ir noteiktas dažādos politikas plānošanas dokumentos (tostarp nozaru dokumentos).

A.1. Politikas plānošanas dokumenti, kas attiecas uz kiberdrošību, tostarp kibernoziedzību

A.1.1. Latvijas Kiberdrošības stratēģija 2014–2018 un tās grozījumi (tostarp rīcības plāns)

Kiberdrošības stratēģijā ir norādīts, ka kibernoziegumu apkarošanas nolūkā ir jāuzlabo ar elektroniskiem pierādījumiem saistītas spējas. Kibernoziedzības izmeklēšana un elektronisko pierādījumu vākšana un izvērtēšana, un izpratne par jēdzienu "*būtisks kaitējums*" prasa specializētas zināšanas, un, lai nodrošinātu likuma spēku kibertelpā, nepieciešams pietiekams kompetences līmenis tiesībsargājošās iestādēs, prokuratūrā un tiesās. Ņemot to vērā, kiberdrošības stratēģijā paredzēta šāda nepieciešamā rīcība.

I. Likumdošanas pasākumi

- Izvērtēt esošo situāciju un nepieciešamos grozījumus tiesību aktos, kas paredz sodāmību par kaitējumu nodarīšanu tādu informācijas sistēmu drošībai vai darbībai, kuras izmanto automatizētai datu apstrādei.
- Veicināt diskusijas un viedokļu apmaiņu par jauniem informācijas un komunikāciju tehnoloģiju (IKT) noziegumu veidiem un tiesiskās bāzes pilnveidošanu saskaņā ar starptautiskajām tendencēm.
- Izstrādāt vienotu mehānismu, ar ko uzskaita noziedzīgus nodarījumus kibertelpā (statistika, kas ietver tiesībaizsardzības iestādes, prokuratūras un tiesas).

II. Spēju veidošanas un mācību pasākumi

- Izvērtēt un pilnveidot esošās elektronisko pierādījumu iegūšanas un analīzes spējas kibernoziegumu izmeklēšanas procesā (attīstot Valsts policijas kompetenci un pilnveidojot sadarbību ar Informācijas tehnoloģiju drošības incidentu novēršanas institūciju (CERT.LV)).
- Izstrādāt mācību metodiskos materiālus par IKT nozari policijas darbinieku, kibernoziegumu procesu virzītāju un tiesnešu zināšanu uzlabošanai.
- Papildus tam īstenot padziļinātu apmācības programmu kibernoziegumu apkarošanas jautājumos.

III. Pasākumi kibernoziedzības novēršanai un apkarošanai

- Valsts policijā izveidot speciālu vienību darbam ar kibernoziedzību.
- Apkarot un izmeklēt kibernoziegumus, izvērtējot un pilnveidojot esošos resursus, procedūras, sadarbības mehānismus un to efektivitāti.

IV. Sabiedrības informēšanas (un prevencijas) pasākumi

- Palielināt izglītības iestāžu un pedagogu kompetenci un to ieguldījumu bērnu un jauniešu izglītošanā IKT kiberdrošības jautājumos (integrējot šos jautājumus izglītības saturā un organizējot attiecīgas mācību aktivitātes, kas veido izpratni par informācijas drošību, privātuma aizsardzību un e-pakalpojumu lietošanu); papildus tam nodrošināt iespējas bērniem un jauniešiem ziņot par pārkāpumiem internetā un saņemt psihologa atbalstu, kā arī organizēt pedagogu sistemātisku tālākizglītību kiberdrošības jautājumos.
- Veidot ērti pieejamus un dažādām vecuma grupām pielāgotus mācību un informatīvos materiālus par kiberdrošību (izmantošanai izglītības iestādēs un interešu grupās).
- (Sadarbībā ar augstskolām un zinātniskajiem institūtiem) izveidot IKT drošības laboratoriju un organizēt zinātniskas konferences par kiberdrošības un kibernoziedzības aktuālajiem jautājumiem.
- Īstenot izglītojošas un informatīvas kampaņas un citus pasākumus vispārējai sabiedrības izpratnes veicināšanai par kiberdrošību, kibernoziedzību un aktuālajiem apdraudējumiem.

V. Starptautiskas sadarbības pasākumi

- Sadarboties ar dažādām starptautiskām organizācijām, kas strādā kibernoziedzības samazināšanas un novēršanas jomā.

A.1.2. Ministru kabineta 2016. gada rīcības plāns, pielikums, 156. darbība

Apmeklējuma laikā tika minēta speciālas vienības izveide Valsts policijā darbam ar kibernoziedzību. Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka jaunās valdības rīcības plāns (ko apstiprināja 3.5.2016.) neparedz speciālas vienības izveidi Valsts policijā darbam ar kibernoziedzību. Tomēr tas ir paredzēts Valsts policijas attīstības koncepcijā (politikas plānošanas dokumentā), ko valdība apstiprināja 6.4.2016.

A.2. Ar kibernoziedzību saistīti nozaru politikas (iekšlietas) plānošanas dokumenti

A.2.1. Valsts policijas stratēģija 2014.–2016. gadam un Valsts policijas 2016. gada daba plāns

Valsts policijas stratēģijā 2014.–2016. gadam ir norādīts, ka jāuzlabo augsto tehnoloģiju izmantošana noziedzīgu nodarījumu apkarošanā.

2016. gada darba plānā ir paredzēts, ka visu veidu kibernoziegumu apkarošana ir viena no četrām galvenajām Valsts policijas prioritātēm. Valsts policijai būtu jācenšas uzlabot Kriminālprocesa likuma noteikumu izpildi (lai vienkāršotu izmeklēšanu un uzlabotu tās efektivitāti).

A.2.2. Organizētās noziedzības novēršanas un apkarošanas plāns 2014.–2016. gadam

Plānā ir paredzēts efektivizēt tiesībaizsardzības iestāžu un attiecīgo valsts drošības iestāžu darbību. Papildus tam ir jāpanāk labāka izpratne un zināšanas par jaunām tendencēm un dinamiku un par organizētās noziedzības (tostarp kibernoziedzības) apdraudējuma līmeni.

A.2.3. Valsts policijas noziedzības prevencijas stratēģija 2014–2017

Stratēģijā iezīmēti galvenie principi, mērķi, stratēģiskās ievirzes, prioritātes un pieejas noziedzības prevencijā (situatīvā prevencija, sociālā prevencija). Stratēģija paredz, ka interneta drošība ir viena no piecām prioritārajām jomām noziedzības prevencijā.

A.3. Citi ar kibernoziedzību saistīti nozaru politikas plānošanas dokumenti

A.3.1. Intelektuālā īpašuma tiesību aizsardzības un nodrošināšanas pamatnostādnes 2015.–2020. gadam

Pamatnostādnēs uzsvērts, ka Valsts policijas sastāvā ir jāizveido specializēta struktūrvienība kibernoziegumu apkarošanai (ietverot autortiesību pārkāpumus).

A.3.2. Bērnu noziedzības novēršanas un bērnu aizsardzības pret noziedzīgu nodarījumu pamatnostādnes 2013.–2019. gadam

Pamatnostādnēs paredzēti preventīvi pasākumi, lai palīdzētu bērniem izvairīties no noziedzības un ziņot par aizdomīgu saturu internetā (piemēram, informācijas kampaņas par drošu interneta lietošanu, uzticības tālruņi).

A.3.3. Cilvēku tirdzniecības novēršanas pamatnostādnes 2014.–2020. gadam

Pamatnostādnes paredz ziņot par gadījumiem, kad, izmantojot interneta sociālos tīklus, tikuši vervēti cietušie vai iespējamie cietušie, kā arī sniegt informāciju par iespējamiem cilvēku tirdzniecības gadījumiem vai mēģinājumiem.

B. Saiknes ar ES politikas ciklu organizētas un smagas starptautiskas noziedzības jomā

Kas attiecas uz ES politikas ciklu organizētas un smagas starptautiskas noziedzības jomā, Latvijas kontekstā Organizētās noziedzības novēršanas un apkarošanas plānā 2014.–2016. gadam ir norādītas šādas ES prioritātes: 1) cilvēku tirdzniecība; 2) krāpšanās akcīzes nodokļa un PVN jomā; 3) sintētiskās narkotikas; 4) heroīns; 5) kibernoziegumi; 6) organizētās noziedzības darbības pret īpašumu.

Latvija piedalās tajās ES prioritātēs, kuras valsts līmenī uz vietas rada vislielāko apdraudējumu, un tajās, kurās Latvijai ir tiešs sakars ar kādu konkrētu parādību (piemēram, cilvēku tirdzniecību), un to stratēģisko mērķu un konkrētu operatīvo rīcības plānu darbību īstenošanā, kas saistīti ar nacionālajām prioritātēm, pasākumiem un darbībām (kā paredzēts Valsts policijas stratēģijā 2014.–2016. gadam, Valsts policijas 2016. gada daba plānā, Organizētās noziedzības novēršanas un apkarošanas plānā 2014.–2016. gadam un Valsts policijas noziedzības prevencijas stratēģijā 2014–2017). Latvija piedalās visos trijos kibernoziedzības apkarošanas operatīvajos rīcības plānos.

3.3. Kibernoziedzības statistika

3.3.1. Galvenās tendences kibernoziedzībā

Galvenās Latvijas iestāžu novērotās tendences kibernoziedzībā 2015. un 2016. gadā ir šādas:

- izspiešana, kas saistīta ar izkliedētā pakalpojumu atteikuma un izspiedējvīrusa uzbrukumiem privātajam sektoram (komersantiem);
- Latvijas mitināšanas iespēju izmantošana – tā kā interneta ātrums Latvijā ir ļoti liels un savienojumu kvalitāte ir ļoti laba, Latvijas interneta savienojumi arvien vairāk tiek izmantoti noziedzīgu nodarījumu pastrādāšanai no ārzemēm (tas jo īpaši attiecas uz bērnu seksuālu izmantošanu un ļaunprogrammatūru); pastāv arī anonimitātes jautājums, un tas būtu jāuzsver (IP adrešu diapazonu tālākpārdošana privātiem interneta pakalpojumu sniedzējiem, kas nav reģistrēti kā elektronisko sakaru komersanti);
- bērnu pornogrāfijas un pedofilisku materiālu izplatīšana internetā (tendence, kas ir attīstījusies ilgākā laikā);
- pikšķerēšanas uzbrukumi un ļaunprogrammatūra;
- ļaunprogrammatūras uzbrukumi banku sistēmām un interneta bankas pakalpojumu lietotājiem;
- "karšu koplietošana" – dalīšanās ar aizsargātām kabeļtelevīzijas dekoderu kartēm vai informāciju par kodu.

2015. gadā Latvijā tika ierosināti kopumā 47 406 kriminālprocesi, no kuriem 453 bija saistīti ar kibernoziedzību. Tātad kibernoziedzība veidoja 0,96 % no visiem kriminālprocesiem. Valsts policija ierosināja 44 900 kriminālprocesus, un no tiem ar kibernoziedzību bija saistīti 427 (jeb 0,95 %). Plašākā kontekstā kibernoziedzība (noziedzīgi nodarījumi, kas izdarīti, izmantojot kibersistēmas, un noziedzīgi nodarījumi, kas saistīti ar kibersistēmām) veido 1,54 % no visiem kriminālprocesiem Latvijā.

3.3.2. Reģistrēto kibernoziedzības gadījumu skaits

Tiesībaizsardzības statistika

Visām tiesībaizsardzības iestādēm ir piekļuve Integrētajai iekšlietu informācijas sistēmai (IIIS) – reģistram, kura pārzinis un turētājs ir Iekšlietu ministrijas Informācijas centrs. IIIS ir vairākas apakšsistēmas, tostarp Sodu reģistrs, kas cita starpā satur datus par ierosinātajiem kriminālprocesiem, noziedzīgajiem nodarījumiem un apsūdzētajām personām, kā arī konkrētu informāciju par kriminālprocesiem (no KRASS). Informāciju sniedz amatpersonas, kuras saskaņā ar Kriminālprocesa likumu pilnvarotas veikt kriminālprocesu. Autorizētiem lietotājiem ir tieša piekļuve IIIS.

Iekšlietu ministrijas Informācijas centrs pārzina un uztur arī Kriminālprocesa informācijas sistēmu (KRASS), kas satur informāciju par uzsāktajiem kriminālprocesiem, konstatētajiem noziedzīgajiem nodarījumiem, procesa virzītājiem, personām, kurām ir tiesības uz aizstāvību, un cietušajiem. Ziņas KRASS sistēmā ievada tiešsaistes režīmā ne vēlāk kā nākamajā darbdienā pēc procesuālās darbības veikšanas, fakta reģistrēšanas vai tiesas nolēmuma stāšanās spēkā.

Tieslietu statistika

Tieslietu statistiku glabā atsevišķi no tiesībaizsardzības statistikas.

Tiesu informatīvo sistēmu (TIS) uztur Tieslietu ministrija. Tās uzdevums ir atvieglot reģistrēšanu, glabāt un apstrādāt tieslietu informāciju, apmainīties ar to un savākt statistikas datus. Tieslietu statistika ir pieejama tiesībaizsardzības iestādēm.

Latvijas iestādes informēja, ka nav iespējams iegūt pilnīgu datu kopumu (no kriminālprocesa ierosināšanas līdz ziņām par notiesāšanu) vienā informācijas sistēmā. Tomēr daļa sistēmu ir savienotas (piemēram, TIS ir savienota ar KRASS, lai nodrošinātu datu apmaiņu, izņemot statistiku, un KRASS ir saistīta ar IIIS Sodu reģistru).

Privātā sektora loma

Privātais sektors statistiku par kibernoziedzību nepapildina. Tomēr CERT.LV vāc statistikas datus, kuru pamatā cita starpā ir privātā sektora iesniegtie dati.

Jāņem vērā, ka ierosinātie kriminālprocesi (krimināllietas, ko Valsts policija iesniegusi Prokuratūrai kriminālvajāšanas nolūkā) var netikt pabeigti viena vai divu gadu laikā; līdz ar to, piemēram, 2015. gadā taisīts galīgais spriedums var būt par noziedzīgu nodarījumu, kas reģistrēts pirms 2014. gada.

Krimināl-likums	Ierosinātie kriminālprocesi (kopā) [23]		Valsts policijas ierosinātie kriminālprocesi		Reģistrētie noziedzīgie nodarījumi		Krimināllietas, ko Valsts policija iesniegusi Prokuratūrai kriminālvajāšanas nolūkā		Galīgais spriedums	
	2015	2014	2015	2014	2015	2014	2015	2014	2015	2014
78. panta otrā daļa [24]	8	10	0	0	8	7	0	0	6	7
144. pants [25]	9	12	7	6	8	21	1	4	1	0
148. pants [26]	41	37	35	35	34	34	26	23	4	9
166. pants [27]	84	48	82	47	226	82	29	27	17	10
177.[1] pants [28]	60	52	59	52	67	60	14	14	3	10
193.[1] pants [29]	248	220	240	212	385	484	146	115	23	40
241. pants [30]	1	2	2	1	1	1	0	1	0	0
243. pants [31]	1	1	1	1	1	1	0	0	1	0
244. pants [32]	1	2	1	2	1	2	0	0	0	0
244.[1] pants [33]	0	0	0	0	0	0	0	0	0	0

[23] Latvijas Republikas Valsts policijas, Drošības policijas un Prokuratūras ierosināto kriminālprocesu kopskaits.
[24] Nacionālā, etniskā un rasu naida izraisīšana.
[25] Korespondences un pa elektronisko sakaru tīkliem pārraidāmās informācijas noslēpuma pārkāpšana.
[26] Autortiesību un blakustiesību pārkāpšana.
[27] Pornogrāfiska priekšnesuma demonstrēšanas, intīma rakstura izklaides ierobežošanas un pornogrāfiska rakstura materiāla aprites noteikumu pārkāpšana.
[28] Krāpšana automatizētā datu apstrādes sistēmā.
[29] Datu, programmatūras un iekārtu iegūšana, izgatavošana, izplatīšana, izmantošana un glabāšana nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem.
[30] Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai.
[31] Automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju.
[32] Nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm.
[33] Datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām.
[34] Nacionālā, etniskā un rasu naida izraisīšana.

3.4. Kibernoziedzības novēršanai un apkarošanai piešķirtais iekšējais budžets un ES finansējuma atbalsts

Tā kā kibernoziedzības novēršanā un apkarošanā ir iesaistītas vairākas Valsts policijas struktūrvienības, tieši kibernoziedzībai veltītu budžeta piešķīrumu nav. Ar personāla un tehniskajiem resursiem un citiem jautājumiem saistītas vajadzības tiek finansētas no attiecīgajām Valsts policijas vispārējā budžeta pozīcijām.

ES finansē divu gadu projektu par kibernoziedzības novēršanas un apkarošanas spēju veidošanu, kuru paredzēts sākt 2017. gada aprīlī. Projekts ir viena no Iekšējās drošības fonda nacionālajām prioritātēm. Šo finansējumu (paredzams, ka tas sasniegs EUR 865 775) plānots izmantot tehniskā aprīkojuma iegādei (piemēram, lai nodrošinātu arī attālinātu ekspertīzi), tiesu ekspertu un citu amatpersonu apmācībai un preventīvām darbībām, tostarp informētības veicināšanai (aptverot plašu interešu grupu loku).

3.5. Secinājumi

- Latvija ir pieņēmusi Kiberdrošības stratēģiju un rīcības plānu tās īstenošanai. Stratēģijā ir paredzēta virkne soļu, kas tiek veikti ar mērķi uzlabot Latvijas esošās rīcībspējas kibernoziedzības apkarošanā. Stratēģijā ir paredzēti pieci galvenie virzieni, kuros jāpanāk uzlabojumi, proti: likumdošanas pasākumi; spēju veidošanas un mācību pasākumi; pasākumi kibernoziedzības novēršanai un apkarošanai (ar mērķi Valsts policijā izveidot kibernoziedzības kontaktpunktu un uzlabot esošās procedūras un sadarbības mehānismus); sabiedrības informēšanas pasākumi; starptautiskas sadarbības pasākumi (ar mērķi uzlabot sadarbību ar dažādām starptautiskām organizācijām).

- Aizsardzības ministrija atbild par Kiberdrošības stratēģijas īstenošanu, koordinē IT drošības un aizsardzības politikas veidošanu un īstenošanu un atbild par starptautisko sadarbību. Tomēr par kibernoziedzības apkarošanu atbild tikai Iekšlietu ministrija (skatīt informāciju par Valsts policiju).

- Galvenās tendences, ko Latvijas iestādes sakarā ar kibernoziedzību novēroja 2015. un 2016. gadā, ir šādas: izspiešana, kas saistīta ar izkliedētā pakalpojumu atteikuma un izspiedējvīrusa uzbrukumiem privātajam sektoram (komersantiem); Latvijas mitināšanas iespēju izmantošana; bērnu pornogrāfijas un pedofilisku materiālu izplatīšana internetā (tendence, kas ir attīstījusies ilgākā laikā); pikšķerēšanas uzbrukumi un ļaunprogrammatūra; ļaunprogrammatūras uzbrukumi banku sistēmām un interneta bankas pakalpojumu lietotājiem; "karšu koplietošana".

- Par lielāko daļu kibernoziedzības kategorijā ietilpstošo vai ar to saistīto noziedzības veidu izmeklēšanu atbild Valsts policija, taču viena kibernoziedzības veida izmeklēšana ir nošķirta un uzticēta Drošības policijai – tā ir "naida runa" jeb rasistisku un ksenofobisku materiālu izplatīšana IT sistēmās. Izvērtēšanas grupa tika informēta, ka tam pamatā ir vēsturisks konteksts un tas, ka valsts ir jāaizsargā pret ārējiem uzbrukumiem no radikālu Latvijas neatkarības pretinieku puses.

- Tomēr statistikas dati rāda, ka 2014. un 2015. gadā ir reģistrēts ļoti maz naida noziegumu, un šķiet, ka vēl mazāk šādu gadījumu ir faktiski iesniegti prokuratūrā. Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka 2016. gadā bija vērojams būtisks naida noziegumu pieaugums.

- Turklāt izvērtējuma apmeklējuma laikā satiktie praktiķi minēja, ka šajā ziņā pastāv problēmas ar Valsts policijas un Drošības policijas jurisdikcijas nodalījumu. Šķiet, ka skaidrāks jurisdikcijas nodalījums nāktu par labu un palielinātu šā kibernoziedzības veida kriminālvajāšanas efektivitāti.

4. VALSTS STRUKTŪRAS

4.1. Tiesu iestādes (prokuratūra un tiesas)

4.1.1. Iekšējā struktūra

a) Tiesas

Satversmes 82. pants paredz, ka tiesu Latvijā spriež rajona (pilsētas) tiesas, apgabaltiesas un Augstākā tiesa, bet kara vai izņēmuma stāvokļa gadījumā – arī kara tiesas.

Latvijā nav speciālu (ārkārtēju) tiesu. Likuma "Par tiesu varu" 1. panta piektajā daļā ir precizēts, ka "nav pieļaujama speciālu (ārkārtēju) tiesu izveidošana, kuras neievēro ar likumu noteiktās procesuālās normas un aizstāj šā panta trešajā daļā minētās tiesas". Tātad Latvijā noziedzīgus nodarījumus kibersistēmās un tādus, kas izdarīti, izmantojot kibersistēmas, izskata parastas rajona (pilsētas) tiesas un apgabaltiesas, kā arī Augstākā tiesa.

Kibernoziedzības lietās specializētu tiesnešu nav.

b) Prokuratūra

Saskaņā ar Prokuratūras likuma 1. pantu prokuratūra ir tiesu varas institūcija, kas patstāvīgi veic uzraudzību pār likumības ievērošanu šajā likumā noteiktās kompetences ietvaros. Prokuratūru veido Ģenerālprokuratūra; tiesu apgabalu prokuratūras; rajonu (pilsētu) prokuratūras; specializētās prokuratūras; un Administratīvā direktora dienests. Kibernoziedzības lietās specializētu prokuroru nav.

Ar kibernoziedzību (proti, nodarījumiem kibersistēmās un tādiem, kas izdarīti, izmantojot kibersistēmas) saistītās pilnvaras

Kibernoziedzība	**Struktūra, kas uzrauga pirmstiesas izmeklēšanu, veic kriminālvajāšanu un uztur valsts apsūdzību**
Kibernoziedzība Rīgas tiesu apgabalā (ietverot Krimināllikuma 241., 243., 244., 244.[1] un 245. pantu)	Finanšu un ekonomisko noziegumu izmeklēšanas prokuratūra
Kibernoziedzība, kuras mērķis vai izdarīšanas rīks ir datorsistēma vai IT sistēma (Krimināllikuma 177.[1] panta trešā daļa)	Organizētās noziedzības un citu nozaru specializētā prokuratūra
Citi kibernoziegumi	Vispārējās jurisdikcijas prokuratūra

4.1.2. Sekmīgas kriminālvajāšanas spējas un šķēršļi

Latvijas iestādes uzsvēra, ka Prokuratūra īpašu uzmanību pievērš prokuroru apmācībai un ka šajā sakarā tiks darīts vairāk. Lai uzlabotu prokuroru spējas, viņiem ir pieejamas Latvijā un ārzemēs organizētas mācības.

2014. un 2015. gadā prokurori piedalījās šādos mācību pasākumos:

- "Kibernoziedzība" (organizators: Prokuratūra sadarbībā ar Latvijas Tiesnešu mācību centru; 54 dalībnieki);
- "Kibernoziedzība un elektroniskie pierādījumi" (organizators: Prokuratūra sadarbībā ar Latvijas Tiesnešu mācību centru; 57 dalībnieki);
- "Kiberdrošības krīžu pārvarēšana" (organizators: CERT.LV; viens dalībnieks);
- "Kibernoziedzības tiesiskie un tehniskie aspekti" (organizators: Eiropas tiesību akadēmija (*ERA*), Trīre, Vācija; trīs dalībnieki);

- "Elektronisko pierādījumu meklēšanas un izņemšanas plānošana un pamatojums: praktiskie jautājumi praktizējošiem juristiem kriminālprocesos pirms pierādījumu iesniegšanas tiesā" (organizators: Eiropas tiesību akadēmija sadarbībā ar Latvijas Tiesnešu mācību centru; pieci dalībnieki);
- "Kibernoziedzības juridisko un tehnisko aspektu pamatkurss" (organizators: Eiropas tiesību akadēmija, Trīre, Vācija; divi dalībnieki);
- "Digitālais pirātisms – izmeklēšana un kriminālvajāšana" (Ungārija; viens dalībnieks).

Prokuratūra ir apzinājusi šādus galvenos šķēršļus un grūtības:

- elektronisko sakaru komersantiem ir pienākums nodrošināt datu glabāšanu 18 mēnešus, kā arī šo datu nodošanu attiecīgām institūcijām (tostarp Prokuratūrai), bet dažās sarežģītās un ilgstošās lietās 18 mēneši ir pārāk īss datu glabāšanas laiks;
- anonīmu interneta pakalpojumu sniegšana (priekšapmaksas internets, Wi-Fi, viena IP adrese vairākām ierīcēm);
- elektronisko sakaru komersantu nespēja laikus iesniegt prasīto informāciju;
- iespēja, ka vienu IP adresi izmanto tūkstoši lietotāju dienā (vienošanās par IP adreses lietošanu);
- ilgi kavējas infotehnisko ekspertīžu rezultātu saņemšana (jo Latvijā trūkst ekspertu un esošie eksperti ir pārslogoti);
- ir ļoti ierobežotas iespējas laikus saņemt ārpus Latvijas reģistrētas IP adreses.

4.2. Tiesībaizsardzības iestādes

Par kibernoziedzības novēršanu un apkarošanu ir atbildīgas šādas Valsts policijas struktūrvienības:

- Galvenā kārtības policijas pārvalde: kibernoziedzības prevencija;
- Galvenā kriminālpolicijas pārvalde: kibernoziedzības apkarošana.

a) Prevencija

Prevencijas vadības nodaļa, kas ir Galvenās kārtības policijas pārvaldes sastāvā, atbild par noziedzības prevencijas koordināciju un īstenošanu. Prevencijas vadības nodaļā četri policisti strādā tieši ar preventīvu pasākumu īstenošanu šādās jomās: 1) narkotikas; 2) vardarbība (skolā un ģimenē); 3) mantiski nodarījumi; 4) kibernoziegumi. Šie policisti katrs savā jomā atbild par to, lai uzlabotu sadarbību ar attiecīgajām valsts un pašvaldību iestādēm, NVO un citām ieinteresētajām personām, kā arī lai iegūtu papildu finansējumu.

Prevencijas vadības nodaļa ir izveidojusi labu sadarbību ar attiecīgajām Galvenās kriminālpolicijas pārvaldes struktūrvienībām, piemēram, ar Ekonomisko noziegumu apkarošanas pārvaldi, kas informē Prevencijas vadības nodaļu par jauniem pavērsieniem un citiem nozīmīgiem jautājumiem sakarā ar kibernoziedzību. Ir plānots arī palielināt pilsoniskās sabiedrības iesaisti, izmantojot Valsts policijas 2016. gadā uzsākto brīvprātīgo programmu, kuras ietvaros brīvprātīgie stāsta un izplata sabiedrībai informāciju par virkni aktuālu jautājumu, tostarp par interneta drošību.

Papildus tam konkrēti prevencijas pasākumi tiek veikti piecu reģionālo pārvalžu līmenī (dažādās jomās specializēti policijas inspektori).

Galvenās kārtības policijas pārvaldes organigramma:

b) Kibernoziedzības apkarošana

Galvenajā kriminālpolicijas pārvaldē ir piecas struktūrvienības. Divas no tām tieši strādā kibernoziedzības apkarošanā:

- Ekonomisko noziegumu apkarošanas pārvalde;
- Starptautiskās sadarbības birojs.

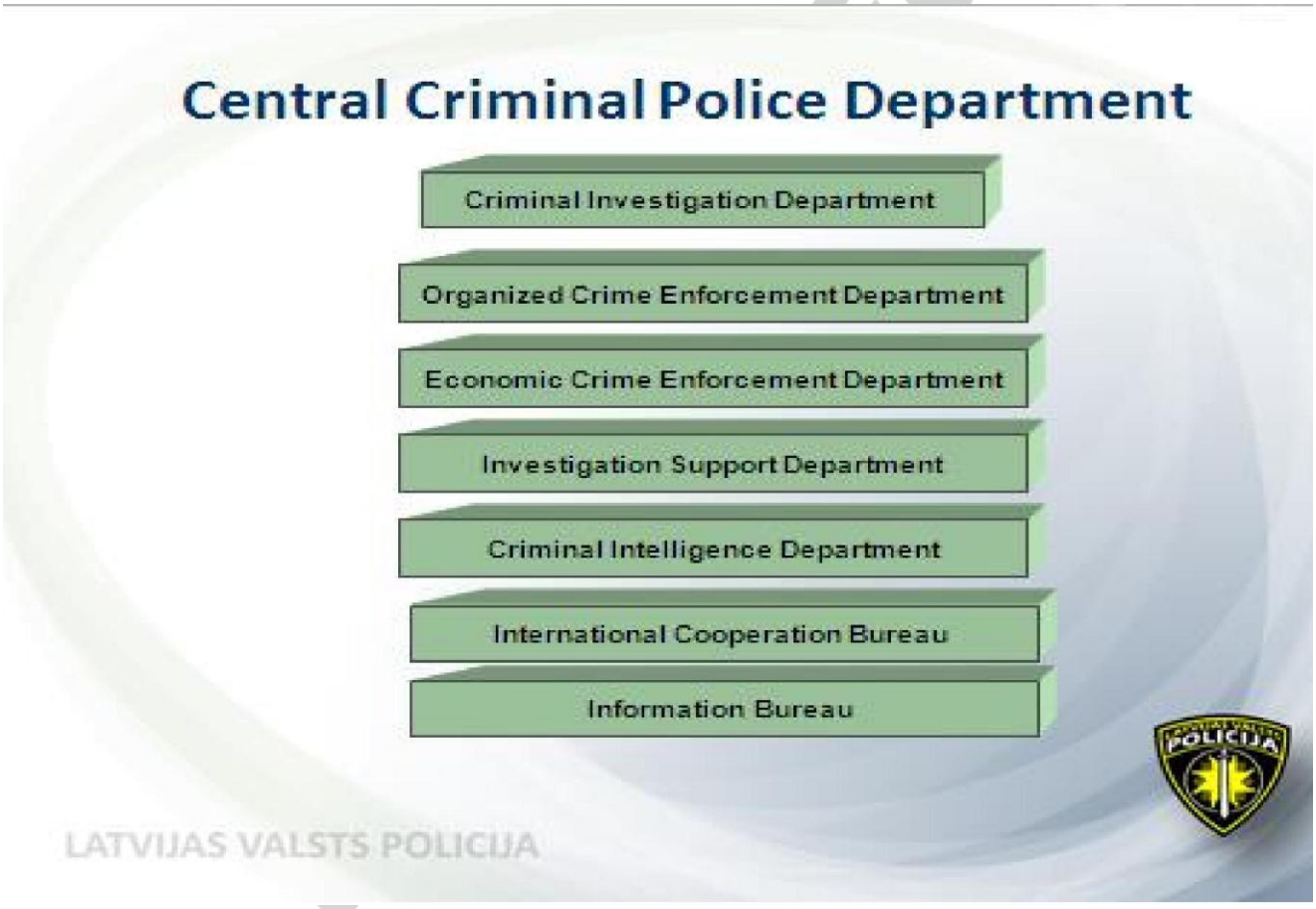
Ekonomisko noziegumu apkarošanas pārvaldei ir četras nodaļas:

- 1. nodaļa: Informācijas un finanšu analīzes grupa;
- 2. nodaļa: Noziedzīgu nodarījumu bankās un kredītiestādēs apkarošana;
- 3. nodaļa: Cīņa ar krāpšanu, naudas viltošanu un nelicencētu uzņēmējdarbību;
- 4. nodaļa: Kibernoziegumu apkarošana.

Kibernoziegumu apkarošanas nodaļā kopā ir 13 policisti. Viņu uzdevumi sadalīti šādi: noziegumu pret automatizētām datu apstrādes sistēmām apkarošana (trīs policisti); operatīvās analīzes grupa (viens policists); tehniskais atbalsts, interneta izlūkošana, bērnu seksuālā izmantošana tiešsaistē (divi policisti); intelektuālā īpašuma aizsardzība (divi policisti); izmeklēšana (trīs policisti).

Saskaņā ar nesenajiem grozījumiem Ministru kabineta noteikumos Nr. 568 par Iekšlietu ministrijas sistēmas iestāžu algām un piemaksām (2015. gada 7. aprīlis) amatpersonām, kas strādā kibernoziedzības apkarošanas jomā, atkarībā no individuālā veikuma var piešķirt piemaksu līdz 400 euro apmērā. [7]

Galvenās kriminālpolicijas pārvaldes organigramma:



[7] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka, sākot ar 2017. gada janvāri, Kibernoziegumu apkarošanas nodaļa (3. nodaļa, iepriekš – 4. nodaļa) nodarbojas arī ar krāpnieciskiem darījumiem tiešsaistē un krāpnieciskiem darījumiem ar maksājumu kartēm, kā arī ar rūpnieciskā īpašuma jautājumiem. Darbinieku kopējais skaits ir palielinājies; Kibernoziegumu apkarošanas nodaļā šobrīd strādā 20 amatpersonas. Ir paaugstinātas arī amatpersonu dienesta pakāpes un saglabāta piemaksu sistēma. Turklāt katram apgabalam (5) ir izraudzīta kontaktpersona/atbalsta darbinieks; tie darbojas Kibernoziegumu apkarošanas nodaļas "pakļautībā", kurai ir tiesības lūgt atbalstu konkrētos prioritāros jautājumos.

Infotehnisko ekspertīžu nodaļa ir Valsts policijas Kriminālistikas pārvaldes daļa. Kas attiecas uz cilvēkresursiem, apmeklējuma laikā Infotehnisko ekspertīžu nodaļā pieņēma darbā četrus sertificētus ekspertus, kuri palīdz izmeklētājiem. Šiem ekspertiem ir augstākā izglītība IT jomā.

2015. gada rudenī sāka veidot IT speciālistu grupu. Tās uzdevums ir nodrošināt augstas kvalitātes atbalstu izmeklētājiem, pirms tiek noteikta ekspertīze. Apmeklējuma laikā Infotehnisko ekspertīžu nodaļas eksperti apmācīja divus speciālistus. Tika plānots 2016. gada beigās grupu vēl paplašināt (vēl divi speciālisti).

Valsts policija ir apzinājusi šādas galvenās problēmjomas kibernoziedzības apkarošanā: uzlabot Kibernoziegumu apkarošanas nodaļas spējas un apmācību; tehniskās spējas un aprīkojums (piemēram, pierādījumu fiksēšanai uz vietas); strauja tehnoloģiju attīstība (piemēram, šifrēšanā); satura infotehniskā ekspertīze (īpaši sarežģīti jautājumi ir ļaunprogrammatūra un kiberuzbrukumi; CERT.LV kā speciālisti sniedz vērtīgu ieguldījumu, kuru tomēr nevar izmantot kā pierādījumus krimināprocesā, jo saskaņā ar Kriminālprocesa likumu "par pierādījumu kriminālprocesā var būt eksperta [...] atzinums par faktiem un apstākļiem, kuru rakstveidā sniedz konkrētajā kriminālprocesā iesaistīts eksperts [...]"); infotehnisko ekspertīžu ilgums (tiesu ekspertīzi parasti veic viena līdz divu mēnešu laikā).

Operatīvais 24/7 kontaktpunkts ir Valsts policijas Galvenās kriminālpolicijas pārvaldes Starptautiskās sadarbības biroja Operatīvās koordinācijas un informatīvā nodrošinājuma nodaļa. Šī nodaļa darbojas kā "apkalpošanas nodaļa" tiesu iestāžu starptautiskai sadarbībai krimināllietās, nodrošinot vienotu kontaktpunktu un nepārtrauktā režīmā koordinējot visu starptautisko informācijas apmaiņu (Interpols, Eiropols, *SIRENE*, sadarbība krimināllietās, kibernoziedzības kontaktpunkts). Tādā veidā Latvija ir izveidojusi vienotu kontaktpunktu, visus policijas starptautiskās sadarbības dienestus iekļaujot kopīgā datu saņemšanas un apstrādes plūsmā.

Operatīvās koordinācijas un informatīvā nodrošinājuma nodaļā ir 16 darbinieki: desmit operatīvie dežuranti, četri policisti (darba laikā veic administratīvus uzdevumus) un viena civilpersona (strādā ar starptautiskiem projektiem). Kontaktpunktā par operatīvajiem dežurantiem strādā tikai policisti (10 policisti maiņu darbā).

Galvenie kontaktpunkta uzdevumi ir šādi:

- nepārtrauktā režīmā dalīties un apmainīties ar informāciju starp Latvijas un ārvalstu tiesībaizsardzības iestādēm;
- palīdzēt Latvijas un ārvalstu tiesībaizsardzības iestādēm organizētās noziedzības, kibernoziedzības un nelikumīgas imigrācijas apkarošanā un novēršanā;
- veikt personu identifikāciju, dokumentu pārbaudi, meklēšanā esošu un pazudušu personu meklēšanu, zagtu transportlīdzekļu un priekšmetu meklēšanu;
- koordinēt pārrobežu noziegumu novēršanā un izmeklēšanā iesaistītās iestādes, ietverot policijas sadarbību Šengenas konvencijas (piemēram, 40. un 41. panta) ietvaros;
- vispārēja policijas sadarbība (Šengenas konvencijas 39. pants);
- Zviedrijas iniciatīva (Padomes Pamatlēmums 2006/960/TI);
- procedūra pēc trāpījuma Prīmes sistēmā.

Kontaktpunkta policistiem ir izmeklēšanas pilnvaras, un viņi piemēro jebkādus izmeklēšanas pasākumus saistībā ar darbībām kriminālllietās. Papildus tam viņi vāc elektroniskos pierādījumus saistībā ar dažādiem nodarījumu veidiem. Lielākā daļa kontaktpunkta policistu ir apmeklējuši Valsts policijas koledžas organizēto pamatkursu "Jaunākās tehnoloģijas policijas darbā".

4.3. Citas iestādes / struktūras / publiskā-privātā partnerība

Papildus tiesu iestādēm un tiesībaizsardzības iestādēm būtu jāuzsver šādu struktūru loma kibernoziedzības novēršanā un apkarošanā:

- Nacionālā IT drošības padome;
- CERT.LV;
- Drošāka interneta centrs *Net-Safe Latvia*.

Nacionālā IT drošības padome

Tā ir centrālā platforma informācijas apmaiņai un sadarbībai starp publiskām iestādēm un privātām struktūrām. Tajā ir pārstāvji no dažādām iestādēm, tādām kā Aizsardzības ministrija, Latvijas Banka, Tieslietu ministrija, Finanšu un kapitāla tirgus komisija u. c. (Plašāka informācija 4.4.1. punktā.)

CERT.LV

Kopš 2011. gada 1. februāra CERT.LV ir uzticēts veicināt IT drošību Latvijā. Šī institūcija darbojas Aizsardzības ministrijas pakļautībā, un tās pilnvaras reglamentē IT drošības likums. Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu IT drošības incidentu novēršanā, konsultēt valsts iestādes un organizēt informatīvus un izglītojošus pasākumus valsts iestāžu darbiniekiem, IT drošības profesionāļiem un sabiedrībai.

CERT.LV sniedz atbalstu arī Informācijas tehnoloģiju un informācijas sistēmu drošības ekspertu grupai (DEG) un drošākas interneta vides iniciatīvai "Atbildīgs IPS", un tā uztur tīmekļa vietni esidross.lv, kas paredzēta plašai sabiedrībai un sniedz padomus par to, kā aizsargāt datorus un rūpēties par savu drošību internetā.

Drošāka interneta centrs *Net-Safe Latvia*.

Drošāka interneta centrs *Net-Safe Latvia* (Centrs) ir ES *Safer Internet* programmas *Insafe* tīkla nacionālais kontaktpunkts Latvijā. Tā galvenie uzdevumi ir šādi: informēt un izglītot (mērķa grupas: bērni, pusaudži, skolotāji un vecāki); ziņot par nelikumīgu tiešsaistes saturu un pārkāpumiem (ziņojumi ir anonīmi; tos apstrādā un vajadzības gadījumā nosūta Valsts policijai izmeklēšanai); nodrošināt Valsts bērnu tiesību aizsardzības inspekcijas uzticības tālruņa 116111 darbību (plašāka informācija 6.2.3. punktā).

4.4. Sadarbība un koordinācija valsts līmenī

4.4.1. Juridiskās vai politiskās saistības

Kā norādīts Kiberdrošības stratēģijā, IT drošības un aizsardzības politikas veidošanu un īstenošanu koordinē Aizsardzības ministrija, kas ir atbildīga arī par starptautisko sadarbību. Līdz ar to kiberdrošības kā tādas kontekstā Aizsardzības ministrijai ir galvenā koordinējošā loma. Tomēr par kibernoziedzības apkarošanu atbild tikai Iekšlietu ministrija (galvenokārt Valsts policija un konkrētos gadījumos arī Drošības policija).

Valsts policijas atbildībā ir apkarot nodarījumus pret datorizētu datu un datorsistēmu konfidencialitāti, neaizskaramību un pieejamību (nelikumīga piekļuve, nelikumīga pārtveršana, iejaukšanās datos, iejaukšanās sistēmās, ļaunprātīga ierīču izmantošana); ar datoriem saistītus nodarījumus (ar datoriem saistīta viltošana, datorkrāpšana); ar saturu saistītus nodarījumus (ar bērnu pornogrāfiju saistīti pārkāpumi); un ar autortiesību un blakustiesību pārkāpšanu saistītus nodarījumus.

Drošības policijas atbildībā ir apkarot rasistisku un ksenofobisku materiālu izplatīšanu datorsistēmās.

Kibernoziedzības prevencijas pasākumos ir iesaistītas vairākas ministrijas:

- Iekšlietu ministrija (Valsts policija, Drošības policija) galvenokārt strādā ar sabiedrības informēšanu un kampaņām (tādos jautājumos kā jaunas tendences kibernoziedzībā, riski un iespējas no tiem izvairīties);
- Izglītības un zinātnes ministrija savas kompetences ietvaros veicina informētību un izpratni par kibertelpu un tās drošu lietošanu;
- Labklājības ministrija īsteno sociālo politiku un bērnu tiesību aizsardzības politiku.

Koordinācijas pamatā ir savstarpējas sadarbības princips, katrai iestādei vai struktūrai savu funkciju izpildē vai nu tieši, vai caur Nacionālo IT drošības padomi (Padomi) sadarbojoties ar pārējiem iesaistītajiem. Padome tika izveidota ar IT drošības likumu, un tā ir arī centrālā platforma informācijas apmaiņai un sadarbībai starp publisko un privāto sektoru. Padomes darbību nodrošina Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļa. Padomes darbā piedalās šādas iestādes un struktūras:

1) Aizsardzības ministrija;
2) Ārlietu ministrija;
3) Finanšu un kapitāla tirgus komisija;
4) Latvijas Banka;
5) Ekonomikas ministrija;
6) Iekšlietu ministrija, Valsts policija un Drošības policija;
7) CERT.LV;
8) Izglītības un zinātnes ministrija;
9) Labklājības ministrija;
10) Drošāka interneta centrs *Net-Safe Latvia*;
11) Valsts kanceleja;

12) Nacionālie bruņotie spēki un Zemessardzes Kiberaizsardzības vienība;

13) IT nozares NVO;

14) Satiksmes ministrija;

15) Satversmes aizsardzības birojs;

16) Tieslietu ministrija un Datu valsts inspekcija;

17) valsts akciju sabiedrība "Latvijas Valsts radio un televīzijas centrs";

18) Vides aizsardzības un reģionālās attīstības ministrija.

Kas attiecas uz koordināciju, Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļa regulāri informē Ministru kabinetu (iesniedzot progresa ziņojumus) un Saeimu par Kiberdrošības stratēģijas īstenošanas gaitu. Tādā veidā Saeima īsteno savas uzraudzības funkcijas šajā jomā. Saeima ir visai aktīva un izvirza virkni aktuālu jautājumu, tostarp sakarā ar sadarbību starp dažādām valsts struktūrām (piemēram, nesen tika aicināts pastiprināt sadarbību starp Kiberaizsardzības vienību Zemessardzē (kas ietilpst Nacionālajos bruņotajos spēkos) un attiecīgo Valsts policijas struktūrvienību).

4.4.2. Sadarbības uzlabošanai piešķirtie resursi

Valsts policija plaši izmanto *CEPOL*, Eiropola un citu struktūru piedāvātās apmācību iespējas, lai uzlabotu policistu spējas. Apmācībās piedalās arī tiesu eksperti. Tomēr Latvijas iestādes norāda, ka šīs apmācības būtu jāpadara intensīvākas, jo IT joma strauji attīstās.

Kas attiecas uz maksājumu karšu un skimeru nelikumīgas izmantošanas izmeklēšanu, tika ziņots, ka Infotehnisko ekspertīžu nodaļai (Valsts policijas Kriminālistikas pārvalde) ir vajadzīgie tehniskie un personāla resursi. Tomēr tika atzīmēts, ka ir jāuzlabo Kibernoziegumu apkarošanas nodaļas izmantotais tehniskais aprīkojums (proti, programmatūra un tehniskie resursi), kā arī zināšanas par jaunākajām tehnoloģijām. Izmantojot esošos resursus, tiek mēģināts uzlabot sadarbību ar privāto sektoru.

4.5. Secinājumi

- Satversmes 82. pants paredz, ka pastāv rajona (pilsētas) tiesas, apgabaltiesas un Augstākā tiesa. Latvijā nav speciālu tiesu kibernoziedzības lietām. Tās izskata parastās tiesas. Tiesneši dalās pieredzē par konkrētiem lietu veidiem, izmantojot e-pastu organizētās grupās. Arī centralizētā judikatūras datubāze, kurā pieejami tiesas nolēmumi, ļauj tiesnešiem būt informētiem par citu tiesu pieņemtajiem nolēmumiem, un tas palīdz nodrošināt taisnīgu tiesas spriešanu un juridisko noteiktību.

- Tomēr tiesneši atzinīgi vērtētu iespēju apmainīties ar informāciju par to, kā rīkoties sarežģītākajās kibernoziedzības lietās, īpaši tādās, kurām ir starptautiska dimensija. Izvērtētāji uzskata, ka efektīvai tiesas spriešanai par labu nāktu, ja tiktu izveidots tādu tiesnešu tīkls, kuriem ir attiecīga pieredze sarežģītu kibernoziedzības lietu izskatīšanā ES līmenī.

- Prokuratūra ir tiesu varas institūcija, kas patstāvīgi veic uzraudzību pār likumības ievērošanu likumā noteiktās kompetences ietvaros. Prokuratūra nav Nacionālās IT drošības padomes locekle.

- Prokuratūra ir iesaistīta darbā ar kibernoziedzības lietām (piemēram, Finanšu un ekonomisko noziegumu izmeklēšanas prokuratūra, Organizētās noziedzības prokuratūra un Ģenerālprokuratūra). Šķiet, ka ar lielāko daļu kibernoziedzības lietu strādā tiesu apgabalu prokuratūras. Tomēr kibernoziedzības lietās specializētu prokuroru nav. Tāpēc izvērtētāji uzskata, ka būtu jāapsver specializācijas iespējas prokuratūrā, piemēram, katrā tiesu apgabalā ieceļot prokuroru, kas specializējas kibernoziedzības lietās, vai visiem prokuroriem izdodot iekšējas pamatnostādnes par kriminālpolitiku sakarā ar kibernoziedzību vai par kriminālprocesa jautājumiem, piemēram, par elektronisko pierādījumu iegūšanu (mobilo tālruņu pārmeklēšana, meklēšana tīklā, slepenas operācijas internetā).

- Par kibernoziedzības apkarošanu atbild Valsts policija un Drošības policija. Valsts policijā par kibernoziedzības prevenciju atbild Galvenā kārtības policijas pārvalde, bet par tās apkarošanu – Galvenā kriminālpolicijas pārvalde.

- Tā kā kibernoziedzībai ir dažādi veidi, Valsts policijā ar to strādā vairākas struktūrvienības: Kriminālizmeklēšanas pārvalde, Ekonomisko noziegumu apkarošanas pārvalde un Starptautiskās sadarbības birojs. Arī šajās dažādajās struktūrvienībās atbildība ir sadalīta starp vairākām nodaļām.

- Apmeklējuma laikā Latvijas valdības rīcības plānā bija paredzēts Valsts policijā izveidot atsevišķu vienību kibernoziedzības apkarošanai. Šobrīd tas ir paredzēts Valsts policijas attīstības koncepcijā. Izvērtētāji to uzskata par nozīmīgu soli ierobežotu policijas spēju uzlabošanai kibernoziedzības jomā. Tomēr papildu resursiem vajadzētu padarīt iespējamu to, ka šai centrālajai nodaļai būtu operatīvās un tehniskās spējas autonomi strādāt ar vissarežģītākajiem kibernoziedzības veidiem (piemēram, ielaušanos aizsargātos tīklos, organizēto noziedzību), kā arī ievērojamas spējas sniegt atbalstu reģionālām policijas struktūrvienībām darbā ar ierastākiem kibernoziedzības veidiem. Tātad būtu jādomā par to, kā uzturēt un palielināt Valsts policijas resursus un līdz ar to stiprināt valsts spējas kibernoziedzības apkarošanā. Būtu jādomā arī par to, kā policijā izveidot pietiekamas izlūkošanas spējas sakarā ar kiberdraudiem un noziedzīgiem grupējumiem kibernoziedzības jomā. Tāpēc uzslavējams ir mērķis racionalizēt un vienkāršot dažādo Valsts policijas struktūrvienību struktūru un to funkciju sadalījumu, lai panāktu vislabāko iespējamo ieguldījumu atdevi. Ļoti rūpīgi būtu jāapsver iespēja atbildību par kibernoziedzību koncentrēt vienā Valsts policijas struktūrvienībā, kam konkrētu atbalstu sniegtu Infotehnisko ekspertīžu nodaļa.

- Ekspertīžu pusi izmeklēšanā nodrošina Infotehnisko ekspertīžu nodaļa, kuras atbildībā ir arī sniegt atbalstu ar IT saistītos jautājumos visām pārējām Valsts policijas struktūrvienībām, kā arī Militārajai policijai, tiesām un citām Valsts policijā neietilpstošām struktūrām. Ņemot vērā kibernoziedzības apkarošanai atvēlēto resursu trūkumu, šķiet, ka būtu jānosaka skaidras prioritātes, lai reģionālo policijas struktūrvienību līmenī veidotu ekspertīžu pamatspējas (piemēram, mobilo tālruņu analīzei) un atslogotu Valsts policijas Infotehnisko ekspertīžu nodaļu, un ļautu tai savus ierobežotos resursus koncentrēt uz sarežģītākiem kriminālekspertīzes jautājumiem. Izvērtētāji uzskata, ka būtisks ir pietiekams un moderns tehniskais aprīkojums (gan iekārtas, gan programmatūra), lai ierobežotos personāla resursus varētu izmantot pēc iespējas efektīvāk.

- Izvērtēšanas grupa tika informēta, ka, neraugoties uz ierobežotajiem finanšu resursiem Valsts policijā, kibernoziedzības jomā strādājošiem policistiem tiek piešķirtas piemaksas pie algas. Izvērtētāji to uzskata par labu praksi, jo tādā veidā tiek atbalstīti zinoši un prasmīgi darbinieki un tas palīdz viņus noturēt darbā.

- Valsts policijas Informācijas birojs ir izveidojis automatizētu sistēmu saziņai ar iekšzemes interneta pakalpojumu sniedzējiem, izmantojot veidlapas un vienotu kontaktpunktu, lai nodrošinātu, ka digitālu pierādījumu datu pieprasījumi tiek efektīvi izpildīti. Sistēma novērš pārpratumus, kavējumus un neskaidrības policistu un interneta pakalpojumu sniedzēju starpā un nodrošina ātras un precīzas atbildes uz pieprasījumiem, kas dažkārt ir steidzami.

- Nacionālā IT drošības padome kalpo kā platforma saziņai starp valsts iestādēm un nevalstiskām struktūrām, kuras atbild par Latvijas Kiberdrošības stratēģijas īstenošanu. Padomei gan nav pilnvaru dot "rīkojumus" saviem locekļiem, bet tā darbojas kā nozīmīgs koordinācijas un diskusiju forums. Tajā tiek apspriesta politika un tās īstenošana, tiek izstrādāti un kopīgi apstiprināti vienoti risinājumi. Turklāt pārstāvji, kas tikās ar izvērtēšanas grupu, apliecināja, ka jebkādas domstarpības var viegli pacelt politiskā līmenī, kur tās var salīdzinoši ātri atrisināt un risinājumus var īstenot. Tas ir tāpēc, ka Padomes darbā ir iesaistīta Saeima. Tā kā kibernoziedzības novēršanā ir iesaistītas vairākas ministrijas, spēja ātri un efektīvi koordinēt politiku un vajadzības gadījumā ātri panākt politisku konsensu šķiet īpaši svarīga. Tomēr izvērtētāji uzskata, ka Latvijai būtu vairāk jāizmanto esošās struktūras un kanāli, lai uzlabotu koordināciju.

- Tāpēc Nacionālajai IT drošības padomei būtu optimāli jāizmanto savas spējas un varas pozīcija, cita starpā palielinot privātā sektora ieinteresēto personu iesaisti koordinācijas procesā. Nacionālajai IT drošības padomei būtu jāapsver iespēja konkrētos koordinācijas projektos – piemēram, prevencijas jomā – iesaistīt konkrētus privātā sektora partnerus, lai novērstu robus vai pārklāšanos kibernoziedzības apkarošanā.

- Ļoti nozīmīga loma Latvijas kibernoziedzības apkarošanas stratēģijā ir CERT.LV. Šī institūcija visām valsts struktūrām, kas darbojas šajā jomā, nodrošina ļoti vērtīgas zināšanas un darbojas kā svarīgs partneris visās visvairāk skartajās jomās privātajā sektorā. Tā novēro visus kiberincidentus un piedāvā arī testēšanas un tehniskas mācības, lai palielinātu kiberdrošību un atvieglotu kibernoziedzības prevenciju. Tā arī aktīvi piedalās mācībās un sadarbībā starptautiskā līmenī, piemēram, NATO un *Cyber Europe* (*ENISA* vadītās) mācībās. CERT.LV arī aktīvi darbojas prevencijas un informēšanas darbā gan sabiedrības, gan IT jomas profesionāļu vidū. Izvērtētāji uzskata, ka CERT.LV šķiet ļoti efektīva un elastīga organizācija, kas spēj pielāgoties strauji mainīgajai kiberdrošības videi un nodrošināt visām attiecīgajām publiskā un privātā sektora struktūrām tik ļoti vajadzīgo atbalstu.

5. TIESISKIE ASPEKTI

5.1. Materiālās krimināltiesību normas, kas attiecas uz kibernoziedzību

5.1.1. Eiropas Padomes Konvencija par kibernoziegumiem

Latvija 2007. gada 1. jūnijā pilnībā ieviesa Konvenciju par kibernoziegumiem un tās Papildu protokolu par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās.

5.1.2. Valsts likumdošanas apraksts

A) Padomes Pamatlēmums 2005/222/TI par uzbrukumiem informācijas sistēmām un Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām

Padomes Pamatlēmums 2005/222/TI par uzbrukumiem informācijas sistēmām un Direktīva 2013/40/ES Latvijas tiesību sistēmā ir transponēti ar grozījumiem šādos aktos:

- Krimināllikums, tostarp 2014. gada 25. septembrī pieņemtie Krimināllikuma grozījumi (144., 241., 243. un 244. pants);
- Krimināllikuma spēkā stāšanās un piemērošanas kārtība;
- Kriminālprocesa likums;
- Operatīvās darbības likums;
- Latvijas administratīvo pārkāpumu kodekss;
- Elektronisko sakaru likums;
- Informācijas sabiedrības pakalpojumu likums;

- Informācijas tehnoloģiju drošības likums;
- Fizisko personu datu aizsardzības likums;
- Pornogrāfijas ierobežošanas likums;
- Bērnu tiesību aizsardzības likums;
- likums "Par tiesu varu";
- Prokuratūras likums.

Krimināllikumā ir daudz normu par kibernoziedzību [8]. Tajā ir noteikta krimināltbildība par šādiem nodarījumiem: nelikumīga pārtveršana (144. pants); datu, programmatūras un iekārtu iegūšana, izgatavošana, izplatīšana, izmantošana un glabāšana nelikumīgām darbībām ar finanšu instrumentiem un maksāšanas līdzekļiem (193.[1] pants); patvaļīga piekļūšana automatizētai datu apstrādes sistēmai (241. pants); automatizētas datu apstrādes sistēmas darbības traucēšana un nelikumīga rīcība ar šajā sistēmā iekļauto informāciju (243. pants); nelikumīgas darbības ar automatizētas datu apstrādes sistēmas resursu ietekmēšanas ierīcēm (244. pants); datu, programmatūras un iekārtu iegūšana, izgatavošana, izmainīšana, glabāšana un izplatīšana nelikumīgām darbībām ar elektronisko sakaru tīklu galiekārtām (244.[1] pants).

Likums paredz, ka sodāmi ir arī mēģinājumi izdarīt šādas darbības. Latvijas tiesībās ir noteikta krimināltbildība arī par kūdīšanu un atbalstīšanu. Juridiskas personas, tostarp valsts vai pašvaldību kapitālsabiedrības, kā arī partnerības, var būt saucamas pie krimināltbildības par noziedzīgiem nodarījumiem, kas izdarīti, veicot to darbības, to interesēs vai labā.

Krimināllikumā nav dota kibernoziedzības definīcija. Tiek runāts par noziedzīgiem nodarījumiem, kas izdarīti automatizētās datu apstrādes sistēmās, un tādiem, kas izdarīti, izmantojot automatizētas datu apstrādes sistēmas (nodarījumi ar tiešsaistes elementu).

[8] Lielā teksta apjoma dēļ šajā ziņojumā nav iekļauts apraksts. Plašāka informācija ir D pielikumā.

B) Direktīva 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu

Latvija ir pilnībā transponējusi Direktīvu 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, veicot grozījumus Krimināllikumā (48., 159.–162.[1], 164.–166. pants). To rezultātā tika noteikta krimināltbildība par pamudināšanu iesaistīties seksuālās darbībās (162.[1] pants) un par pornogrāfiska priekšnesuma demonstrēšanas, intīma rakstura izklaides ierobežošanas un pornogrāfiska materiāla aprites noteikumu pārkāpšanu (166. pants) [9].

Latvija norādīja, ka tai ir progresīvs tiesiskais regulējums attiecībā uz pornogrāfiju un tāpēc nav nozīmīgu problēmu ar kvalificēšanu. Piemēram, atšķirībā no citām valstīm Latvijā bija iespējams ierosināt kriminālprocesu "Šreka" pornogrāfijas lietā par pornogrāfiska rakstura skaņas ierakstu / runu / animācijas filmu. Pornogrāfijas ierobežošanas likums paredz, ka "pornogrāfiska rakstura materiāls" ir "sacerējums, iespieddarbs, attēls, datorprogramma, filma, video vai skaņu ieraksts, televīzijas raidījums vai radioraidījums, cits materiāls jebkurā formā vai veidā [..]".

C) Krāpnieciski darījumi ar norēķinu kartēm tiešsaistē

Lai sodītu par krāpnieciskiem darījumiem ar norēķinu kartēm tiešsaistē, ir paredzēta krimināltbildība par šādiem nodarījumiem.
Nelikumīgas darbības ar fiziskās personas datiem (145. pants)
Par *nelikumīgām darbībām ar fiziskās personas datiem*, ja ar to radīts būtisks kaitējums, soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu (145. panta pirmā daļa).

[9] Lielā teksta apjoma dēļ šajā ziņojumā nav iekļauts apraksts. Plašāka informācija ir D pielikumā.

Par *nelikumīgām darbībām ar fiziskās personas datiem*, ja tās izdarījis personas datu apstrādes pārzinis vai operators atriebības, mantkārīgā vai šantāžas nolūkā, soda ar brīvības atņemšanu uz laiku līdz četriem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu (145. panta otrā daļa).

Par *personas datu apstrādes pārziņa vai operatora vai datu subjekta ietekmēšanu*, pielietojot vardarbību vai draudus vai ļaunprātīgi izmantojot uzticību, vai ar viltu nolūkā veikt nelikumīgas darbības ar fiziskās personas datiem soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu (145. panta trešā daļa).

Krāpšana automatizētā datu apstrādes sistēmā (177.[1] pants), ja persona svešas mantas vai tiesību uz šādu mantu, vai citu mantisku labumu iegūšanai apzināti ievada automatizētā datu apstrādes sistēmā nepatiesus datus, lai ietekmētu tās resursu darbību (datorkrāpšana) (177.[1] panta pirmā daļa):

- par *datorkrāpšanu, ja to izdarījusi personu grupa pēc iepriekšējas vienošanās*, soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu, konfiscējot mantu vai bez mantas konfiskācijas (177.[1] panta otrā daļa);

- par *datorkrāpšanu, ja tā izdarīta lielā apmērā vai ja to izdarījusi organizēta grupa*, soda ar brīvības atņemšanu uz laiku no diviem līdz desmit gadiem, konfiscējot mantu vai bez mantas konfiskācijas, un ar probācijas uzraudzību uz laiku līdz trim gadiem vai bez tās (177.[1] panta trešā daļa).

D) Citas kibernoziedzības izpausmes

Krimināllikuma 78. panta otrā daļa (nacionālā, etniskā un rasu naida izraisīšana): par šādiem nodarījumiem [*darbību, kas vērsta uz nacionālā, etniskā, rasu vai reliģiskā naida vai nesaticības izraisīšanu*], ja to izdarījusi personu grupa vai valsts amatpersona, vai uzņēmuma (uzņēmējsabiedrības) vai organizācijas atbildīgs darbinieks vai *ja tā izdarīta, izmantojot automatizētu datu apstrādes sistēmu*, soda ar brīvības atņemšanu uz laiku līdz pieciem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu.

88. panta otrajā daļā (terorisms) minēts datorterorisms: par valsts teritorijā vai kontinentālajā šelfā izvietotu fizisku objektu, *automatizēto datu apstrādes sistēmu, elektronisko tīklu*, kā arī citu objektu iznīcināšanu vai bojāšanu, ja šādas darbības veiktas 88. panta pirmajā daļā paredzētajā nolūkā, soda ar mūža ieslodzījumu vai brīvības atņemšanu uz laiku no astoņiem līdz divdesmit gadiem, konfiscējot mantu vai bez mantas konfiskācijas, un ar probācijas uzraudzību uz laiku līdz trim gadiem.

148. pants (autortiesību un blakustiesību pārkāpšana):

- Par *autortiesību vai blakustiesību pārkāpšanu*, ja ar to radīts *būtisks kaitējums ar likumu aizsargātām personas interesēm*, soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu (panta pirmā daļa);
- par 148. panta pirmajā daļā paredzēto noziedzīgo nodarījumu, *ja to izdarījusi personu grupa pēc iepriekšējas vienošanās*, soda ar brīvības atņemšanu uz laiku līdz četriem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu (panta otrā daļa);
- par autortiesību vai blakustiesību pārkāpšanu, *ja tā izdarīta lielā apmērā vai ja to izdarījusi organizēta grupa, vai par piespiešanu ar vardarbību, draudiem vai šantāžu atteikties no autorības, vai par līdzautorības uzspiešanu, ja tā izdarīta ar vardarbību, draudiem vai šantāžu*, soda ar brīvības atņemšanu uz laiku līdz sešiem gadiem, atņemot tiesības uz noteiktu nodarbošanos uz laiku līdz pieciem gadiem, un ar probācijas uzraudzību uz laiku līdz trim gadiem vai bez tās (panta trešā daļa).

182. pants (elektroenerģijas, siltumenerģijas un gāzes patvaļīga patērēšana, elektronisko sakaru pakalpojumu patvaļīga izmantošana):

- par elektroenerģijas, siltumenerģijas vai gāzes patvaļīgu patērēšanu vai par *elektronisko sakaru pakalpojumu patvaļīgu izmantošanu*, ja ar to radīts *ievērojams mantisks zaudējums*, soda ar īslaicīgu brīvības atņemšanu vai ar piespiedu darbu, vai ar naudas sodu;
- par elektroenerģijas, siltumenerģijas vai gāzes patvaļīgu patērēšanu vai par elektronisko sakaru pakalpojumu patvaļīgu izmantošanu, ja tas izdarīts *lielā apmērā* vai *ja to izdarījusi personu grupa pēc iepriekšējas vienošanās*, soda ar brīvības atņemšanu uz laiku līdz diviem gadiem vai ar īslaicīgu brīvības atņemšanu, vai ar piespiedu darbu, vai ar naudas sodu.

245. pants (informācijas sistēmas drošības noteikumu pārkāpšana):

- par *saskaņā ar informācijas režīmu vai tās aizsardzību izstrādātu informācijas glabāšanas un apstrādes noteikumu vai citu informācijas datorsistēmas drošības noteikumu pārkāpšanu, ko izdarījusi persona, kura ir atbildīga par šo noteikumu ievērošanu*, ja tas bijis par iemeslu informācijas nolaupīšanai, iznīcināšanai vai bojāšanai vai ja ar to radīts cits *būtisks kaitējums*, soda ar īslaicīgu brīvības atņemšanu vai ar piespiedu darbu, vai ar naudas sodu.

Latvijas Administratīvo pārkāpumu kodeksa 204.[16] pants paredz, ka par likumā noteiktā komerciāla paziņojuma (tā dēvēto "surogātpasta" vēstuļu jeb "mēstuļu") sūtīšanas aizlieguma pārkāpšanu izsaka brīdinājumu vai uzliek naudas sodu fiziskajām personām no simt četrdesmit līdz piecsimt *euro*, bet juridiskajām personām – no septiņsimt līdz septiņtūkstoš simt *euro*. Kompetentā uzraudzības iestāde ir Datu valsts inspekcija.

5.2. Procesuālie jautājumi

5.2.1. Izmeklēšanas paņēmieni

Kratīšana un izņemšana *(vispārīgi)*

Kriminālprocesa likuma 179. pantā ir paredzēts, ka "*kratīšanu* izdara nolūkā atrast kriminālprocesā nozīmīgus priekšmetus, dokumentus, līķus vai meklējamās personas". 180.–185. pantā ir sīkāk precizēta procedūra un citi attiecīgi jautājumi. 186. pantā ir norādīts, ka "*izņemšana* ir izmeklēšanas darbība, kuras saturs ir lietai nozīmīgu priekšmetu vai dokumentu atņemšana, ja izmeklēšanas darbības veicējam ir zināms, kur vai pie kā atrodas konkrētais priekšmets vai dokuments un tos nav nepieciešams meklēt vai arī tie atrodas publiski pieejamās vietās".

Procesa virzītāja pieprasīto priekšmetu un dokumentu iesniegšana

Kriminālprocesa likuma 190. pantā ir paredzēts, ka procesa virzītājs, neizdarot 186. pantā paredzēto izņemšanu, ir tiesīgs "rakstveidā *pieprasīt* no fiziskajām un juridiskajām personām kriminālprocesam nozīmīgus priekšmetus, dokumentus un ziņas par faktiem, tai skaitā elektroniskas informācijas vai dokumenta formā, kas apstrādātas, uzglabātas vai pārraidītas, izmantojot elektroniskās informācijas sistēmas".

Turklāt, "ja fiziskās un juridiskās personas neiesniedz procesa virzītāja pieprasītos priekšmetus un dokumentus viņa noteiktajā termiņā, procesa virzītājs [..] [Kriminālprocesa] likumā noteiktajā kārtībā izdara izņemšanu vai kratīšanu".

Kā arī "juridisko personu vadītājiem pēc procesa virzītāja pieprasījuma ir pienākums savas kompetences ietvaros izdarīt dokumentālo revīziju, inventarizāciju, resorisko vai dienesta pārbaudi un noteiktajā laikā iesniegt dokumentus kopā ar attiecīgajiem pielikumiem par izpildīto pieprasījumu".

Datu saglabāšana

Kriminālprocesa likuma 191. pantā par elektroniskās informācijas sistēmā esošo datu saglabāšanu ir paredzēts, ka "procesa virzītājs [...] *var uzdot elektroniskās informācijas sistēmas īpašniekam, valdītājam vai turētājam* (tas ir, fiziskajai vai juridiskajai personai, kura ar elektroniskās informācijas sistēmām apstrādā, uzglabā vai pārraida datus, tai skaitā elektronisko sakaru komersantam) *nekavējoties nodrošināt tā rīcībā esošo noteiktu, izmeklēšanas vajadzībām nepieciešamu datu (kuru saglabāšana nav noteikta ar likumu) veseluma saglabāšanu neizmainītā stāvoklī un to nepieejamību citiem informācijas sistēmas lietotājiem*".
Turklāt "datu saglabāšanas pienākumu var noteikt uz laiku līdz *30 dienām*, bet šo termiņu, ja nepieciešams, vēl uz laiku līdz 30 dienām var pagarināt izmeklēšanas tiesnesis".

Saglabāto datu atklāšana un izsniegšana

Elektroniskajā informācijas sistēmā saglabāto datu atklāšanu un izsniegšanu Kriminālprocesa likuma 192. pants reglamentē šādi:

- *pirmstiesas kriminālprocesā* – izmeklētājs "ar prokurora vai ar datu subjekta piekrišanu un prokurors ar amatā augstāka prokurora vai ar datu subjekta piekrišanu var pieprasīt, *lai elektronisko sakaru komersants* atklāj un izsniedz Elektronisko sakaru likumā noteiktajā kārtībā saglabājamos datus";
- *pirmstiesas kriminālprocesā* – "procesa virzītājs, pamatojoties uz izmeklēšanas tiesneša lēmumu vai ar datu subjekta piekrišanu *var* rakstveidā *pieprasīt*, lai elektroniskās informācijas sistēmas īpašnieks, valdītājs vai turētājs atklāj un izsniedz šā likuma 191. pantā paredzētajā kārtībā saglabātos datus";
- *iztiesājot krimināllietu* – "tiesnesis vai tiesas sastāvs var pieprasīt, lai elektronisko sakaru komersants atklāj un izsniedz Elektronisko sakaru likumā noteiktajā kārtībā saglabājamos datus vai elektroniskās informācijas sistēmas īpašnieks, valdītājs vai turētājs atklāj un izsniedz šā likuma 191. pantā paredzētajā kārtībā saglabātos datus".

Sakaru līdzekļu kontrole *(speciāls izmeklēšanas pasākums)*

Kriminālprocesa likuma 218. pantā ir paredzēts, ka "telefonu un citu sakaru līdzekļu kontroli bez sarunas dalībnieku vai informācijas nosūtītāja un saņēmēja ziņas veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka sarunas vai nodotā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem, un ja bez šīs darbības nepieciešamo ziņu iegūšana nav iespējama. Telefonu un citu sakaru līdzekļu kontroli ar sarunas dalībnieka, informācijas nosūtītāja vai saņēmēja rakstveida piekrišanu veic, ja ir pamats uzskatīt, ka pret šo personu vai tās tuviniekiem var tikt vērsts noziedzīgs nodarījums vai arī šī persona ir vai var tikt iesaistīta noziedzīga nodarījuma izdarīšanā."

Automatizētās datu apstrādes sistēmā esošo datu kontrole *(speciāls izmeklēšanas pasākums)*

Kriminālprocesa likuma 219. pantā ir paredzēts, ka "automatizētās datu apstrādes sistēmas (tās daļas), tajā uzkrāto datu, datu vides pārmeklēšanu un piekļuvi tai, kā arī izņemšanu bez šīs sistēmas vai datu īpašnieka, valdītāja vai turētāja ziņas kriminālprocesā veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka konkrētajā sistēmā esošā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem".

Turklāt "izmeklēšanas darbības uzsākšanai procesa virzītājs *var pieprasīt*, lai persona, kura pārzina sistēmas funkcionēšanu vai veic ar datu apstrādi, uzglabāšanu vai pārraidi saistītus pienākumus, sniedz nepieciešamo informāciju, nodrošina sistēmā esošo informācijas un tehnisko resursu veselumu un padara kontrolējamos datus nepieejamus citiem lietotājiem", un "procesa virzītājs var aizliegt šai personai citu darbību veikšanu ar kontrolei pakļautajiem datiem, kā arī brīdina šo personu par izmeklēšanas noslēpuma neizpaušanu". Kā arī "lēmumā par automatizētās datu apstrādes sistēmā esošo datu kontroli izmeklēšanas tiesnesis var atļaut procesa virzītājam izņemt vai citādi saglabāt automatizētās datu apstrādes sistēmas resursus, kā arī izgatavot šo resursu kopijas".

Pārraidīto datu satura kontrole *(speciāls izmeklēšanas pasākums)*

Krimināprocesa likuma 220. pantā ir paredzēts, ka "tādu datu pārtveršanu, vākšanu un ierakstīšanu, kuri pārraidīti ar automatizētās datu apstrādes sistēmas palīdzību, izmantojot Latvijas teritorijā esošās sakaru ierīces (turpmāk – pārraidīto datu kontrole), bez šīs sistēmas īpašnieka, valdītāja vai turētāja ziņas veic, pamatojoties uz izmeklēšanas tiesneša lēmumu, ja ir pamats uzskatīt, ka no datu pārraides iegūtā informācija var saturēt ziņas par pierādāmajos apstākļos ietilpstošajiem faktiem".

5.2.2. Tiesu ekspertīze un šifrēšana

1. Valsts policija

Tiesu ekspertīzi veic Valsts policijas Kriminālistikas pārvaldes Infotehnisko ekspertīžu nodaļa. Tā attiecas gan uz kibernoziedzību, gan citiem noziedzīgiem nodarījumiem, kas saistīti ar elektroniskiem pierādījumiem. Izņemtos priekšmetus analizē laboratorijā. 2014. gadā Infotehnisko ekspertīžu nodaļa veica 290 ekspertīzes, bet 2015. gada pirmajos desmit mēnešos – 200.

Tiesu ekspertīze ietver šādus galvenos uzdevumus: tīkla iestatījumu identificēšana un meklēšana; dzēstu dokumentu atjaunošana; informācijas meklēšana un dzēstas informācijas atjaunošana; dzēstu grafisku failu atjaunošana; grafisku failu un videofailu meklēšana, eksportēšana un atjaunošana (sakarā ar pornogrāfiju, bērnu seksuālu izmantošanu un citiem nodarījumiem); banknošu attēlu meklēšana datu iekārtās; dzēstu elektronisko parakstu meklēšana un atjaunošana; informācijas meklēšana par e-pasta pakalpojumiem (izmantošana, apmeklējumi); vēstures datu eksportēšana (par interneta apmeklējumiem) un dzēstu vēstures datu atjaunošana; failu lejupielādēšanas/augšupielādēšanas apstiprinājumi; kredītkaršu datu meklēšana un atjaunošana; dažādu operētājsistēmu (galvenokārt *Windows*, *Linux*, *Unix* un *Mac OS*) analīze; *Microsoft Windows* operētājsistēmas reģistra analīze; failu atjaunošana; žurnālfailu analīze; failu un konteinerfailu paroļu uzlaušana/noņemšana; ar datu slēpšanas un šifrēšanas programmatūru saistīti uzdevumi; spiegprogrammatūras atklāšana un žurnālu analīze; ar attālās pārvaldības programmatūru saistīti uzdevumi un žurnālfailu analīze; ar vīrusiem saistīti uzdevumi; datu meklēšana (un konvertēšana); magnētisko karšu lasīšanas ierīču (skimeru) (arī pašgatavotu ierīču (skimeru)) analīze; SIM karšu informācijas eksportēšana un atjaunošana; mobilo tālruņu / viedtālruņu atmiņas analīze un informācijas atjaunošana; planšetdatoru analīze; GPS ierīču analīze; digitālo foto/video ierīču datu atjaunošana un analīze; pulšu datu atjaunošana un analīze; paroļu izvilkšana no cietajiem diskiem. Nākotnē Kriminālistikas pārvalde plāno padziļinātāk pievērsties tādiem jautājumiem kā informācijas atjaunošana no bojātām datu iekārtām un informācijas izgūšana no bojātiem mobilajiem tālruņiem / viedtālruņiem un planšetdatoriem.

IT pārbaudē (jeb sākotnējā analīzē pirms tiesu ekspertīzes) tiek veiktas šādas darbības: esošo dokumentu eksportēšana; attiecīgo dokumentu (doc, xls, pdf un citu) meklēšana/atlase (pēc atslēgvārdiem); esošo grafisko failu eksportēšana; e-pasta vēstuļu eksportēšana; tērzēšanas ("čata") sarakstes eksportēšana un atjaunošana.

Valsts policijas Ekonomisko noziegumu apkarošanas pārvalde (4. nodaļa – Kibernoziegumu apkarošana) veic interneta izlūkošanu ("dzīvā/tīkla analīze").

Kas attiecas uz šifrēšanu, Valsts policijas Kriminālistikas pārvaldes Infotehnisko ekspertīžu nodaļai ir vajadzīgais aprīkojums, lai noteiktu šifrēšanas veidu un piekļūtu šifrētai informācijai. Tomēr skaitļošanas spējas ir ierobežotas, un tas liedz šai nodaļai panākt labākus rezultātus (līdz ar to, ja parole ir tehniski sarežģīta un to nevar izgūt saprātīgā laikā, šifrēšanas process tiek izbeigts). Šajā sakarā Latvija saredz skaidru *EC3* šifrēšanas/atšifrēšanas platformas pievienoto vērtību. Šifrēšanas jautājuma kontekstā Latvija augstu vērtē arī Eiropola ekspertu platformas pieejamību. Infotehnisko ekspertīžu nodaļa nesadarbojas ar privātiem uzņēmumiem. Tomēr eksperti var informēt procesa virzītāju, ka ir jāiesaista privātais sektors, lai iegūtu vajadzīgo papildinformāciju.

2. ***Valsts tiesu ekspertīžu birojs (VTEB)***

VTEB ir Tieslietu ministrijas pakļautībā esoša iestāde, kas nodrošina tiesu ekspertīzes pakalpojumus tiesībaizsardzības iestādēm (pēc pieprasījuma), kā arī citām juridiskām un fiziskām personām. Viena no jomām, kurās VTEB piedāvā pakalpojumus, ir informācijas tehnoloģiju/datoru izpēte (piemēram, informācijas meklēšana, dzēstu dokumentu atjaunošana, dokumentu analīze uz cietajiem diskiem, zibatmiņas, kompaktdiskiem un citiem elektroniskiem datu nesējiem).

5.2.3. Elektroniskie pierādījumi

Krimināllikumā ir minēti tādi jēdzieni kā "automatizēta datu apstrādes sistēma", "publiski nepieejami dati" un "elektronisko sakaru tīklu galiekārtas", tomēr tie nav definēti. Elektronisko sakaru likumā ir definēti šādi jēdzieni: elektronisko sakaru komersants, elektronisko sakaru pakalpojums, elektronisko sakaru pakalpojumu sniedzējs, elektronisko sakaru tīkls, piekļuve, galiekārtas, identificējama galiekārta, galalietotājs, piekļuve datu plūsmai, noslodzes dati, atrašanās vietas dati, atrašanās vietas informācijas datubāze, saglabājamie dati.

Kriminālprocesa likuma 136. pantā ir paredzēts, ka "par pierādījumu kriminālprocesā var būt ziņas par faktiem elektroniskas informācijas formā, kas apstrādāta, uzglabāta vai pārraidīta ar automatizētas datu apstrādes ierīcēm vai sistēmām". Turklāt 135. panta otrajā daļā, kas attiecas uz jēdzienu "*dokuments*", ir paskaidrots, ka "par dokumentiem pierādījuma nozīmē [...] uzskatāmi arī datorizētās informācijas nesēji, ar skaņu un attēlu fiksējošiem tehniskiem līdzekļiem izdarīti ieraksti [...]".

Kas attiecas uz praktisko kārtību un paraugpraksi sakarā ar elektroniskajiem pierādījumiem, Valsts policijā ir izveidots vienots kontaktpunkts, kas atbild par vajadzīgo datu pieprasīšanu un saņemšanu no elektronisko sakaru komersantiem (tas nozīmē, ka ir izveidota centralizēta sadarbība starp Valsts policiju un elektronisko sakaru komersantiem). Šim nolūkam ir izstrādāta speciāla datubāze. Vienotais kontaktpunkts ir pieejams nepārtraukti un saņem pieprasījumus no visām Valsts policijas pārvaldēm (katrā reģionālajā Valsts policijas struktūrvienībā ir noteikta kontaktpersona).

Kriminālprocesa likuma 130. pantā par *pierādījumu pieļaujamību* (kas attiecas arī uz elektroniskajiem pierādījumiem) ir paredzēts, ka "kriminālprocesa laikā iegūtās ziņas par faktiem ir pieļaujams izmantot kā pierādījumus, ja tās iegūtas un procesuāli nostiprinātas [..] [Kriminālprocesa] likumā noteiktajā kārtībā". Turklāt tajā norādīts, ka "par *nepieļaujamām un pierādīšanā neizmantojamām* atzīstamas tādas ziņas par faktiem, kuras iegūtas: 1) izmantojot vardarbību, draudus, šantāžu, viltu vai spaidus; 2) procesuālajā darbībā, ko veikusi persona, kurai saskaņā ar [...] [Kriminālprocesa] likumu nebija tiesību to veikt; 3) pieļaujot [...] [Kriminālprocesa] likumā īpaši norādītos pārkāpumus, kas liedz konkrētā pierādījuma izmantošanu; 4) pārkāpjot kriminālprocesa pamatprincipus".

Papildus tam pantā paredzēts, ka "ziņas par faktiem, kuras iegūtas, pieļaujot citus procesuālos pārkāpumus, uzskatāmas par *ierobežoti pieļaujamām* un var tikt izmantotas pierādīšanā tikai tādā gadījumā, ja pieļautie procesuālie pārkāpumi ir nebūtiski vai var tikt novērsti, tie nevarēja ietekmēt iegūto ziņu patiesumu vai ja to ticamību apstiprina pārējās procesā iegūtās ziņas".

Pieļaujamības noteikumi attiecas arī uz ārpus Latvijas iegūtiem elektroniskajiem pierādījumiem (proti, tādiem, kas ir iegūti saskaņā ar Kriminālprocesa likuma 83. nodaļu "Lūgums ārvalstij par procesuālās darbības veikšanu").

5.3. Cilvēktiesību un pamatbrīvību aizsardzība

Juridiskās prasības

Pamattiesības un pamatbrīvības aizsargā Latvijas Republikas **Satversme**. Tās 89. pantā ir paredzēts, ka valsts atzīst un aizsargā cilvēka pamattiesības saskaņā ar Satversmi, likumiem un Latvijai saistošiem starptautiskajiem nolīgumiem. 96. pantā ir norādīts, ka "ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību"; saskaņā ar 99. pantu "ikvienam ir tiesības uz domas, apziņas un reliģiskās pārliecības brīvību"; un 100. pantā ir paredzēts, ka "ikvienam ir tiesības uz vārda brīvību, kas ietver tiesības brīvi iegūt, paturēt un izplatīt informāciju, paust savus uzskatus", kā arī "cenzūra ir aizliegta".

Konkrētāki aizsardzības pasākumi ir paredzēti **Kriminālprocesa likumā** (skatīt 5.2.1.). **Operatīvās darbības likumā** (5. pantā) turklāt ir paredzēts, ka gadījumā, "ja persona uzskata ka operatīvās darbības subjekts ar savu rīcību ir pārkāpis tās likumīgās tiesības un brīvības, šī persona ir tiesīga iesniegt sūdzību prokuroram, kas, veicis pārbaudi, sniedz atzinumu par operatīvās darbības subjekta amatpersonu rīcības atbilstību likumam, kā arī tā var vērsties tiesā".

Datu valsts inspekcija

Datu valsts inspekcija ir valsts pārvaldes iestāde, kuras atbildībā ir uzraudzīt, lai personas datu aizsardzībā tiktu ievērots Fizisko personu datu aizsardzības likums. Tā darbojas neatkarīgi un autonomi, Tieslietu ministrijas pakļautībā.

Pamattiesību un pamatbrīvību garantijas

Kriminālprocesa likuma 12. pantā ir paredzēts, ka "kriminālprocesu veic, ievērojot starptautiski atzītās cilvēktiesības un nepieļaujot neattaisnotu kriminālprocesuālo pienākumu uzlikšanu vai nesamērīgu iejaukšanos personas dzīvē". Turklāt "cilvēktiesības *var ierobežot* tikai tajos gadījumos, kad to prasa sabiedrības drošības apsvērumi, un tikai [...] [Kriminālprocesa] likumā noteiktajā kārtībā atbilstoši noziedzīgā nodarījuma raksturam un bīstamībai". Kā arī "piemērot ar brīvības atņemšanu saistītu drošības līdzekli, pārkāpt publiski nepieejamas vietas neaizskaramību, korespondences un sakaru līdzekļu noslēpumu drīkst vienīgi ar *izmeklēšanas tiesneša vai tiesas piekrišanu*".

Savukārt "amatpersonai, kura veic kriminālprocesu, ir *pienākums aizsargāt personas privātās dzīves noslēpumu* un komercnoslēpumu" un "ziņas par to drīkst iegūt un izmantot tikai tad, ja tas ir nepieciešams pierādāmo apstākļu noskaidrošanai".

Visbeidzot, minētajā pantā ir arī paredzēts, ka "*fiziskajai personai ir tiesības pieprasīt*, lai krimināllietā netiek iekļautas ziņas par šīs personas pašas vai tās saderinātā, laulātā, vecāku, vecvecāku, bērnu, mazbērnu, brāļu un māsu, kā arī tās personas, ar kuru attiecīgā fiziskā persona dzīvo kopā un ar kuru tai ir kopīga (nedalīta) saimniecība (turpmāk – tuvinieki) privāto dzīvi, komercdarbību un mantisko stāvokli, *ja tas nav nepieciešams krimināltiesisko attiecību taisnīgai noregulēšanai*".

Izmeklēšanas tiesnesis

Latvijā pastāv "izmeklēšanas tiesneša" jēdziens; saskaņā ar Kriminālprocesa likuma 40. pantu izmeklēšanas tiesnesis ir "tiesnesis, kuram rajona (pilsētas) tiesas priekšsēdētājs [..] uzdevis *kontrolēt cilvēktiesību ievērošanu kriminālprocesos"*. Izmeklēšanā un kriminālvajāšanā izmeklēšanas tiesnesis var veikt šādus pasākumus:

- likumā paredzētajos gadījumos lemt par piespiedu līdzekļa piemērošanu;
- lemt par aizdomās turētā un apsūdzētā pieteikumiem par to drošības līdzekļu grozīšanu vai atcelšanu, kuri piemēroti ar izmeklēšanas tiesneša lēmumu;
- izskatīt sūdzības par procesa virzītāja piemēroto drošības līdzekli;
- lemt par procesuālo darbību veikšanu;
- lemt par sūdzībām attiecībā uz tādu noslēpumu neattaisnotu pārkāpšanu kriminālprocesā, kurus aizsargā likums;
- lemt par personas, kurai ir tiesības uz aizstāvību, lūgumu atbrīvot no samaksas par advokāta palīdzības izmantošanu.

Pirmās instances tiesā līdz lietas iztiesāšanas uzsākšanai izmeklēšanas tiesnesis lemj par:

- apsūdzētā pieteikumu attiecībā uz drošības līdzekļu grozīšanu vai atcelšanu;
- prokurora ierosinājumu attiecībā uz drošības līdzekļa izraudzīšanu vai grozīšanu;
- kriminālprocesā iesaistītās personas, kurai ir tiesības iepazīties ar krimināllietas materiāliem, iepazīstināšanu ar speciālo izmeklēšanas darbību materiāliem, kuri netiek pievienoti krimināllietai (pirmdokumentiem).

Bet izmeklēšanas tiesnesim nav atļauts aizstāt procesa virzītāju un uzraugošo prokuroru pirmstiesas kriminālprocesā, dodot norādījumus par izmeklēšanas virzienu un izmeklēšanas darbību veikšanu.

5.4. Jurisdikcija

5.4.1. Kibernoziedzības izmeklēšanai piemērojamie principi

Krimināllikuma 4. pantā (par Krimināllikuma spēku ārpus Latvijas teritorijas) ir paredzēts, ka "*Latvijas pilsoņi, nepilsoņi vai ārzemnieki, kuriem ir pastāvīgās uzturēšanās atļauja Latvijas Republikā*, par citas valsts teritorijā vai ārpus jebkuras valsts teritorijas izdarītu nodarījumu neatkarīgi no tā, vai tas izdarīšanas vietā atzīts par noziedzīgu un sodāmu, saucami pie atbildības Latvijas teritorijā saskaņā ar [..] Krimināllikumu".

"Par citas valsts teritorijā vai ārpus jebkuras valsts teritorijas izdarītu nodarījumu neatkarīgi no tā, vai tas izdarīšanas vietā atzīts par noziedzīgu un sodāmu, ja to izdarījusi fiziskā persona Latvijas Republikā reģistrētas juridiskās personas interesēs, labā vai juridiskās personas nepienācīgas pārraudzības vai kontroles rezultātā, juridiskajai personai var piemērot [..] [Krimināllikumā] paredzētos piespiedu ietekmēšanas līdzekļus."

"Ārzemnieki, kuriem nav pastāvīgās uzturēšanās atļaujas Latvijas Republikā un kuri izdarījuši citas valsts teritorijā smagus vai sevišķi smagus noziegumus, kas vērsti pret Latvijas Republikas vai tās iedzīvotāju interesēm, neatkarīgi no tās valsts likumiem, kuras teritorijā izdarīts noziegums, saucami pie kriminālatbildības saskaņā ar [..] [Krimināllikumu], ja tie nav saukti pie kriminālatbildības vai nodoti tiesai saskaņā ar nozieguma izdarīšanas vietas valsts likumiem."

"Ārzemnieki, kuriem nav pastāvīgās uzturēšanās atļaujas Latvijas Republikā un kuri izdarījuši noziedzīgu nodarījumu citas valsts teritorijā vai ārpus jebkuras valsts teritorijas, neatkarīgi no nodarījuma izdarīšanas vietas valsts likumiem saucami pie atbildības saskaņā ar [..] [Krimināllikumu] Latvijas Republikai saistošos starptautiskajos līgumos paredzētajos gadījumos, ja par šo nodarījumu tie nav saukti pie kriminālatbildības vai nodoti tiesai citas valsts teritorijā."

5.4.2. Jurisdikcijas kolīzijas noteikumi un nosūtīšana Eurojust

Principā jurisdikcijas kolīzijas tiek atrisinātas apspriežoties (saskaņā ar Eiropas Padomes tiesību instrumentiem) un *Eurojust* koordinācijas sanāksmēs. Tomēr jāmin, ka kibernoziedzības jomā Ģenerālprokuratūrā nav bijis šādu gadījumu.

Tātad kibernoziedzības lietu sakarā līdz šim nav tikuši izmantoti noteikumi, kas ir saistīti ar Padomes Pamatlēmumu 2009/948/TI (2009. gada 30. novembris) par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā.

5.4.3. Jurisdikcija attiecībā uz "mākonī" izdarītiem kibernoziegumiem

Latvijā nav konstatētas nekādas konkrētas problēmas vai nav rasti nekādi risinājumi attiecībā uz "mākoņa" jautājumu. Latvija uzskata, ka tā ir globāla problēma, kuru varētu – un vajadzētu – risināt ES līmenī. [10] Līdzīgi kā citās valstīs, ja mākoņpakalpojuma sniedzējs ir reģistrēts Latvijā, izmeklēšanas pasākumus veic saskaņā ar attiecīgajiem valsts tiesību aktiem. Ja pakalpojums ir reģistrēts ārpus Latvijas Republikas krimināl ās jurisdikcijas, izmanto lūgumu par tiesisko palīdzību krimināllietā.

Valsts policija minēja labas sadarbības pieredzi ar *Microsoft* (tā ir saņēmusi pozitīvas atbildes uz vairākiem lūgumiem).

[10] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka Latvija pašlaik veic grozījumu Kriminālprocesa likumā, kas paredz svītrot atsauci uz Latvijas teritoriju (220. pants "Pārraidīto datu satura kontrole", kas ir speciāls izmeklēšanas pasākums). Tas ļautu iegūt datus no "mākoņiem", kas bāzēti ārpus Latvijas. Tādējādi – ja personai ir attiecīgie autorizācijas līdzekļi, būtu jānodrošina, lai kompetentajām iestādēm būtu iespēja iegūt datus, kas pieder minētajai personai (līdz ar to nebūtu nekādas saiknes ar valsti, kurā "mākonis" ir bāzēts).

5.4.4. Latvijas izpratne par kibernoziedzības apkarošanas tiesisko regulējumu

Attiecībā uz kibernoziegumiem un elektroniskiem pierādījumiem (jo īpaši datu glabāšanas pieprasījumiem) izšķiroša nozīme ir piemērota termiņa noteikšanai. Diemžēl vairumā gadījumu lūgumi par tiesisko palīdzību krimināllietās netiek izpildīti pietiekami savlaicīgi (piemēram, viena kibernozieguma gadījumā Valsts policijas nosūtītais lūgums tika izpildīts pēc diviem gadiem). Vispārējs novērojums liecina, ka "lūguma par tiesisko palīdzību krimināllietā" instruments neatbilst faktiskajām izmeklēšanas un kriminālvajāšanas vajadzībām digitālajā laikmetā. Būtu jāpārskata "lūguma par tiesisko palīdzību krimināllietā" instrumenta īstenošanas procedūra, lai ņemtu vērā kibernoziegumus.

5.5. Secinājumi

- Latvija ir ratificējusi Budapeštas Konvenciju. Padomes Pamatlēmums 2005/222/TI par uzbrukumiem informācijas sistēmām un Direktīva 2013/40/ES par uzbrukumiem informācijas sistēmām un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI ir transponēti Krimināllikumā. Tāpēc Konvencijā un ES tiesību aktos paredzētie nodarījumi eksistē valsts tiesību aktos.

- Ir īstenota Eiropas Parlamenta un Padomes Direktīva 2011/93/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu. Krimināl kodeksā ir paredzēta krāpšanas ar kredītkartēm apkarošana.

- Izvērtēšanas grupa tika informēta, ka gan Drošības policija, gan Valsts policija ir tiesīga izmeklēt naida noziegumus (Krimināllikuma 78., 149.[1] un 150. pants). Kriminālprocesa likumā ir paredzēts kompetenču sadalījums. Ja rodas diskusija par kompetenci, izmeklēšanas iestādi nosaka ģenerālprokurors (Kriminālprocesa likuma 387. pants). Tomēr praksē šādu noziegumu izmeklēšanā kompetenču sadalījums starp abiem minētajiem policijas spēkiem reizēm paliek neskaidrs. Bez skaidrākām nostādnēm pastāv risks, ka daži naida noziegumu piemēri nenonāks attiecīgo iestāžu uzmanības lokā.

- Šķiet, ka Tieslietu ministrija sadarbībā ar tiesām aktīvi uzrauga situāciju cīņā pret kibernoziedzību. Tieslietu ministrija apliecināja gatavību vajadzības gadījumā aktīvi pieņemt jaunus noteikumus, lai sekmētu kriminālvajāšanu par kibernoziegumiem.

- Tieslietu ministrijā darbojas divas darba grupas, kuru mērķis ir saukt pie atbildības par noziegumiem, un to darbā piedalās akadēmiskais sektors un valsts advokātu palāta. Darba grupas šobrīd strādā pie priekšlikumiem, kuriem būtu jāveicina ātrāka saukšana pie atbildības par noziegumiem. Tomēr apmeklējuma laikā netika sniegti nekādi konkrēti risinājumi, kā sekmēt kriminālvajāšanu un izmeklēšanu par kibernoziegumiem.

- Elektroniskie pierādījumi ir definēti Kriminālprocesa likuma 136. pantā; tomēr nav nekādu īpašu pieļaujamības noteikumu, kas attiecas uz elektroniskiem pierādījumiem. Uz elektroniskiem pierādījumiem attiecas tie paši noteikumi, ko piemēro papīra dokumentiem. Elektronisko sakaru likumā iekļautas vairākas ar datu pārraidi saistītas definīcijas.

- Praktiķi, kas tikās ar izvērtēšanas grupu, minēja, ka Datu saglabāšanas direktīvas atcelšanai ir bijusi negatīva ietekme uz spēju nodrošināt elektroniskos pierādījumus ES dalībvalstīs. Tika uzsvērts, ka šāda notikumu attīstība ir ļoti negatīvi ietekmējusi Latvijas izmeklēšanas iestāžu spēju izmeklēt kibernoziegumus un citus noziegumus, kad elektroniskie pierādījumi un internets vai telekomunikāciju dati būtiski veicinātu vainīgo sekmīgu identificēšanu. Latvijas iestādes uzskata, ka jauns instruments ES līmenī, ar ko saskaņot datu glabāšanas termiņus, dotu pievienoto vērtību.

- Šifrēšana tiek uzskatīta par problēmu. Valsts policijas Kriminālistikas pārvaldes Infotehnisko ekspertīžu nodaļai ir vajadzīgais aprīkojums, lai noteiktu šifrēšanas veidu un piekļūtu šifrētai informācijai. Tomēr aprēķināšanas spējas ir ierobežotas, kas nodaļai neļauj sasniegt labākus rezultātus.

- Uz vietas veikto apmeklējumu laikā izvērtēšanas grupa tika informēta, ka saskaņā ar vispārpieņemto praksi datoraparatūra, kas satur elektroniskus pierādījumus, tiek fiziski izņemta. Kibernoziegumā cietušajam var būt grūti samierināties ar zaudējumu, ko rada viņa vai viņas digitālā aprīkojuma izņemšana uz izmeklēšanas laiku. Šādas personas to var uztvert kā sekundāru viktimizāciju. Ja tiktu ieviesti valsts tiesību akti, kas attiecas uz digitālo materiālu izņemšanu ar dokumentētas spoguļkopēšanas palīdzību, tas varētu iedrošināt cilvēkus labprātāk sadarboties ar tiesībaizsardzības iestādēm. Tāpēc spoguļkopēšana varētu būt digitālā materiāla nodrošināšanas veids [11].

- Valsts tiesību aktos ir transponēts Padomes Pamatlēmums 2009/948/TI (2009. gada 30. novembris) par jurisdikcijas īstenošanas konfliktu novēršanu un atrisināšanu kriminālprocesā. Līdz šim nav reģistrēti nekādi jurisdikcijas konflikti.

[11] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka Latvijas iestādes un struktūras pārskata likumdošanu un neuzskata par vajadzīgu grozīt Kriminālprocesa likumu. Šis jautājums pašlaik tiek risināts, mainot kompetento iestāžu praksi – atdodot priekšmetu (datoraparatūru) atpakaļ īpašniekam vai likumīgajam valdītājam un izgatavojot digitālā materiāla spoguļkopiju.

6. OPERATĪVIE ASPEKTI

6.1. Kiberuzbrukumi

6.1.1. Kiberuzbrukumu raksturs

CERT.LV ir atbildīga par kiberuzbrukumu uzraudzību Latvijā un vienu reizi ceturksnī publicē ikmēneša statistiku gan par augstas, gan zemas prioritātes kiberincidentiem.

2015. gadā katru mēnesi tika reģistrēti 200–300 augstas prioritātes incidenti un vidēji 50 000 zemas prioritātes incidenti. Saskaņā ar CERT.LV incidentu klasifikāciju, nosakot, vai paziņotais incidents ir augstas prioritātes incidents, tiek izvērtēti tādi elementi kā informācijas avots un skartās iestādes (piemēram, valsts iestādes, kritiskā infrastruktūra). Augstas prioritātes incidentus apstrādā ar roku, turpretim zemas prioritātes incidentus apstrādā automātiski. Par incidentiem vai nu ziņo Valsts policijai, vai arī tie tiek pārvarēti saskaņā ar CERT.LV iekšējām procedūrām.

Uzbrukumi, kas vērsti uz Latvijas kibertelpu, kļūst arvien komplicētāki un tiek pamatīgi plānoti. Kiberuzbrukumu parastie mērķi ir Latvijas finanšu sektors un publiskais sektors. Kiberuzbrukumu spektrs ir ļoti plašs, sākot ar ielaušanos sistēmā līdz pat tīmekļa lapu sabojāšanai, banku Trojas zirgiem, pakalpojumatteices uzbrukumiem un ļoti sarežģītiem un modernizētiem pastāvīgiem uzbrukuma draudiem (*APT*). Šo incidentu un uzbrukumu novēršana ir daļa no CERT.LV parastajiem pienākumiem, un to veic saskaņā ar tās politiku un paraugpraksi.

CERT.LV augstu vērtē informācijas apmaiņu ar citām ES dalībvalstīm, ko veicina Datordrošības incidentu reaģēšanas vienības (*CSIRT*) sadarbība (vai nu divpusēji katrā gadījumā atsevišķi, vai izmantojot tādus *CSIRT* sadarbības formātus kā *TF-CSIRT*). Valsts līmenī CERT.LV lielu nozīmi piešķir sadarbībai ar tiesībaizsardzības un izlūkošanas aģentūrām.

Izvērtēšanas grupa tika informēta par to, ka 2015. gada novembrī tika parakstīts saprašanās memorands starp visu triju Baltijas valstu datorapdraudējumu reaģēšanas (*CERT*) vienībām, apņemoties pastiprināt sadarbību kiberuzbrukumu un IT sistēmu un tīklu aizsardzības jomā.

6.1.2. Mehānisms reaģēšanai uz kiberuzbrukumiem

Vispārējs pārskats par reaģēšanas mehānismu

Saskaņā ar Informācijas tehnoloģiju drošības likuma 4. panta piekto daļu valstij radītu draudu gadījumā Ministru kabinets var nolemt nodot CERT.LV uzdevumus, tiesības un resursus Nacionālajiem bruņotajiem spēkiem. Mazāk bīstamos gadījumos CERT.LV ziņo Aizsardzības ministrijai, kura pēc tam konsultējas ar Nacionālo IT drošības padomi un ziņo Ministru kabinetam, ja ir pieņemti vajadzīgie lēmumi.

Kiberaizsardzības vienība

Ņemot vērā esošos drošības apdraudējumus un bažas, kā arī ierobežotos valsts resursus, 2013. gada jūlijā tika izveidota rezerves vienība – Kiberaizsardzības vienība.
Rezerves kiberaizsardzības spējas tika veidotas gan civiliem, gan militāriem mērķiem. Kiberaizsardzības vienībā darbojas privātā un publiskā sektora IT eksperti, kas vēlas sniegt atbalstu valstij krīzes situācijā (proti, ja Nacionālo bruņoto spēku un CERT.LV spējas liekas nepietiekamas). Kiberaizsardzības vienība tiek veidota, pamatojoties uz Zemessardzi, kas nodrošina juridisko pamatu un procedūras augsti kvalificētu privātā sektora IT ekspertu izmantošanai, lai organizētā veidā izpildītu aizsardzības uzdevumus. Šobrīd Kiberaizsardzības vienības sastāvā ir vairāk nekā 70 brīvprātīgie (tās pilnīgas operatīvās spējas ir 94 brīvprātīgie un četri profesionāli karavīri) [12]. Pašlaik Kiberaizsardzības vienības ietvaros IT eksperti strādā pie tā, lai pilnveidotu zināšanas, organizētu kiberuzbrukuma novēršanas mācības un piedalītos tajās, un nepieciešamības gadījuma sniegtu palīdzību gan publiskajam, gan privātajam sektoram.
Galvenie Kiberaizsardzības vienības uzdevumi ir šādi:

- komplektēt IT ekspertus;
- izstrādāt Kiberaizsardzības vienības attīstības un darba plānu;
- nodrošināt iesaistītajiem zemessargiem sākotnējo militāro un tālāko profesionālo apmācību;

[12] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka brīvprātīgo skaits Kiberaizsardzības vienībā pieaug un šobrīd tajā darbojas vairāk nekā 80 personas.

- plānot, organizēt un nodrošināt dalību valsts un starptautiskos mācību kursos (piemēram, regulāra dalība kiberaizsardzības apmācībā NATO, ES, divpusējos un reģionālos formātos, tostarp NATO Kooperatīvajā kiberaizsardzības izcilības centrā, un regulāras apmācības organizēšana valsts līmenī);
- veikt ekspertīzes sadarbībā ar Nacionālo bruņoto spēku un CERT.LV [13] militārajiem *CERT* ekspertiem, piedalīties jaunu drošības risinājumu testēšanā un izvērtēšanā un sniegt priekšlikumus kiberaizsardzības uzlabošanai;
- sagatavoties un piedalīties NATO, ES vai reģionālajās kiberaizsardzības vienībās vai rezervēs;
- veicināt civilo un militāro sadarbību un publiskās un privātās partnerības kiberaizsardzības jomā;
- IT ekspertu vidū un sabiedrībā veicināt izpratni un zināšanas par kiberdraudiem; iesaistīt Jaunsardzi, lai sekmētu jauniešu izglītību un ieinteresētu tos iesaistīties IT drošības un aizsardzības jomā.

Kritiskā IT infrastruktūra

Katrai kritiskajai IT infrastruktūrai īpašnieks vai likumīgais pārvaldnieks izraugās personu, kas ir atbildīga par IT drošību. Izraudzītā persona sadarbojas ar CERT.LV un Satversmes aizsardzības biroju, lai nodrošinātu kritiskās IT infrastruktūras aizsardzību saskaņā ar Ministru kabineta noteikumiem. Turklāt, lai līdz minimumam samazinātu kiberuzbrukumu draudus un mazinātu to ietekmi, tiek veikti šādi pasākumi: saskaņota IT drošības dokumentācija, riska analīze, situatīvā plānošana, izplatības testēšana un reaģēšana uz incidentiem.

[13] 2016. gada sākumā Aizsardzības ministrija izveidoja arī Militāro datorapdraudējumu reaģēšanas vienību (*MilCERT*), kura cieši sadarbojas ar CERT.LV.

6.2. Pasākumi, kas vērsti pret bērnu pornogrāfiju un seksuālu vardarbību tiešsaistē

6.2.1. Elektroniskas datubāzes cietušo identificēšanai un pasākumi atkārtotas viktimizācijas novēršanai

Latvijai nav valsts elektroniskas datubāzes, kas paredzēta tieši cietušo identificēšanai. Tomēr, lai pastiprinātu tās spēju apkarot nodarījumus, kas saistīti ar seksuālu vardarbību pret bērniem tiešsaistē un bērnu pornogrāfiju, Valsts policija aktīvi izmanto tādas starptautiskas datubāzes un instrumentus kā:

- ***Child Protection System* (Bērnu aizsardzības sistēma) (*CPS*)** – to personu datubāze, kuras regulāri pārkāpj noteikumus par darbībām ar bērnu pornogrāfijas materiāliem (arī Latvijas teritorijā);
- ***Voyager One*** – visaptveroša tīmekļa platforma, kas Valsts policijai ļauj atklāt noziedzīgu organizāciju tīklus, kā arī ļaunprātīgus bērnu izmantotājus;
- ***ICACCOPS*** – uz tīmekli balstīta datubāze, kas ļauj identificēt IP adreses, kurām ir kopīgi nelikumīgi materiāli, kuri tiek augšupielādēti (ir iespējams redzēt *Gnutella*, *Emule*, *IRC*, *Gigatribe*, *TOR*, *Bittorrent* un *Freener* tīkla IP adreses);
- ***Biometric Data Processing System* (Biometrisko datu apstrādes sistēma) (*BDPS*)** – datubāze, kas ietver kriminālprocesos iesaistīto personu – aizdomās turēto, aizturēto un notiesāto personu – biometriskos datus (sejas attēlus, desmit pirkstu nospiedumus, kas iegūti ar uzspiešanas metodi, desmit pirkstu nospiedumus, kas iegūti ar pārvelšanas metodi, un plaukstu nospiedumus). *BDPS* ietver arī salīdzināmus paraugus (bioloģisko materiālu, kas ņemts no cietušajiem un no apcietinātajām, aizdomās turētajām, apsūdzētajām vai notiesātajām personām, kā arī no neidentificētiem ķermeņiem un bezvēsts pazudušo personu bioloģiski tuviem radiniekiem (vecākiem, bērniem), lai noskaidrotu bioloģiskās izcelsmes pēdas), kas Valsts policijai ļauj identificēt bezvēsts pazudušu personu vai neidentificētu ķermeni.

No 2016. gada 30. jūnija Valsts policija arī sāka izmantot Interpola Starptautisko bērnu seksuālas izmantošanas (*ICSE*) datubāzi.

Saskaņā ar Kriminālprocesa likumu (239. panta ceturto daļu) notikuma vietas apskates laikā operācijas veicējs var izņemt priekšmetus ar noziedzīga nodarījuma pēdām (tostarp datoraparatūru). Pēc galīgās notiesāšanas lietiskie pierādījumi (kuru aprite aizliegta ar likumu) ir jānodod attiecīgajām iestādēm vai arī jāiznīcina saskaņā ar procesa virzītāja lēmumu. Datoraparatūra, kas satur attēlus vai video, kuri saistīti ar seksuālu vardarbību pret bērniem tiešsaistē un bērnu pornogrāfiju, vienmēr tiek iznīcināta (ja ne pilnībā – tad daļēji, izdzēšot materiālu ar nelikumīgu saturu).

Lai pilnībā īstenotu Eiropas Parlamenta un Padomes Direktīvu 2012/29/ES (2012. gada 25. oktobris), ar ko nosaka noziegumos cietušo tiesību, atbalsta un aizsardzības minimālos standartus un aizstāj Padomes Pamatlēmumu 2001/220/TI (4. nodaļa: Cietušo aizsardzība un to cietušo atzīšana, kuriem vajadzīga īpaša aizsardzība), pieņemšanai parlamentā tika iesniegti Kriminālprocesa likuma grozījumi. Ir jāievieš jauna nodaļa par cietušajiem, kuriem vajadzīga īpaša aizsardzība, un jāīsteno jauni pasākumi. Tie ietver, piemēram, pasākumus ar mērķi izvairīties no vizuāla kontakta starp cietušajiem un likumpārkāpējiem liecības sniegšanas laikā (izmantojot piemērotus līdzekļus, tostarp komunikācijas tehnoloģiju). Cietušo iztaujāšana būtu jāveic šim nolūkam apmācītiem speciālistiem vai ar viņu starpniecību. Personas, kuras cietušas no seksuālas vardarbības, dzimuma vardarbības vai vardarbības tuvās attiecībās, būtu jāiztaujā tā paša dzimuma personai, ja cietušais tā vēlas (tas neattiecas uz prokuroriem un tiesnešiem). Turklāt ir jāīsteno pasākumi, ar ko nodrošina, ka cietušos tiesas zālē var uzklausīt bez viņu klātbūtnes, jo īpaši izmantojot piemērotu komunikācijas tehnoloģiju.

6.2.2. Pasākumi ar mērķi novērst seksuālu izmantošanu un vardarbību tiešsaistē, sekstingu un kiberiebiedēšanu

Kas attiecas uz seksuālu izmantošanu un vardarbību tiešsaistē un sekstingu, Krimināllikuma 162. pantā ir paredzēta kriminālatbildība par tādām darbībām, ar kurām persona, izmantojot informāciju vai komunikācijas tehnoloģijas vai citus saziņas veidus, pamudina citu 16 gadus nesasniegušu personu iesaistīties seksuālās darbībās vai pamudina šādu personu tikties ar mērķi izdarīt seksuālas darbības vai stāties dzimumattiecībās.

Nav ieviesta nekāda juridiskā definīcija par kiberiebiedēšanu; kiberiebiedēšana kā tāda var būt gan krimināli sodāma, gan krimināli nesodāma rīcība (atkarībā no izraisītajām sekām), un tāpēc katrs gadījums ir izskatīts atsevišķi. Krimināllikumā ir vairāki panti, ko var piemērot kiberiebiedēšanas gadījumos, piemēram, 150. pants "Reliģiska naida izraisīšana", 157. pants "Neslavas celšana" un 145. pants "Nelikumīgas darbības ar fiziskās personas datiem".

6.2.3. Preventīvi pasākumi pret sekstūrismu, bērnu pornogrāfiskiem priekšnesumiem u. c.

Saskaņā ar Pornogrāfijas ierobežošanas likumu (8. pants) pornogrāfiska rakstura materiālu reklamēšana ir aizliegta. Reklamēšana ir ar peļņas gūšanas nolūkā veiktu saimniecisko darbību saistīts jebkuras formas vai veida paziņojums vai pasākums, kura mērķis ir veicināt pornogrāfiska rakstura materiāla popularitāti vai pieprasījumu.

Krimināllikumā nav paredzēta juridiskā definīcija par bērnu sekstūrismu vai tā reklamēšanu. Tomēr praksē, ja persona organizē vai reklamē šādus ceļojumus, viņu var uzskatīt par attiecīgā noziedzīgā nodarījuma izdarītāju saskaņā ar Krimināllikumu (piemēram, 162. pantu).

Praktisko pasākumu kontekstā 2014. gada 17. un 18. septembrī Valsts policija (seši darbinieki), Muitas pārvalde (četri darbinieki) un Valsts Robežsardze (astoņi darbinieki) piedalījās starptautiskajā operācijā *HAVEN* (*Halting Europeans Abusing Victims in Every Nation* – operācija ar mērķi nepieļaut cietušo ļaunprātīgu izmantošanu nevienā Eiropas valstī). Operācijas mērķis bija atbalstīt ES dalībvalstis, palīdzot tām atklāt un aizturēt bērnu seksuālus izmantotājus, kas ceļo nolūkā ļaunprātīgi izmantot bērnus.

Lai novērstu sekstūrismu un bērnu pornogrāfiskus priekšnesumus, ir ieviesti šādi speciāli preventīvi pasākumi:

Uzticības (palīdzības) tālruņi un konkrēta informācija par to, kā reģistrēt sūdzību

Par kibernoziegumiem var ziņot, zvanot uz 112 vai 110 vai aizpildot reģistrācijas veidlapu tiešsaistē. Lai vienkāršotu procedūru, ko var izmantot, lai ziņotu par jebkāda veida noziedzīgiem nodarījumiem, tostarp kibernoziegumiem, visa nepieciešamā informācija ir skatāma Valsts policijas tīmekļa vietnē (pieejama latviešu, angļu un krievu valodā). Sūdzības, kas saistītas ar kibernoziegumiem, var arī iesniegt Drošāka interneta centram *Net-Safe Latvia*, izmantojot uzticības tālruni, vai attiecībā uz kiberuzbrukumiem – CERT. LV.

Bērniem (un vecākiem) paredzēti informācijas instrumenti par drošu interneta lietošanu un kaitīgu vai nelikumīgu rīcību tiešsaistē

1. Valsts policijas pasākumi

Pavisam kopā Valsts policija 2014. gadā organizēja 61 un 2015. gadā – 312 prevencijas iniciatīvas, kas saistītas ar interneta drošību. Cita starpā ar tām rosināja:

- sniegt informāciju par **"desmit svarīgākajiem interneta saziņas noteikumiem"** Valsts policijas tīmekļa vietnē, lai aizsargātu personas, tostarp bērnus, no iespējamiem ļaunprātīgiem izmantotājiem internetā;
- ciešā sadarbībā ar Drošāka interneta centru *Net-Safe Latvia* organizēt **apmācību** par interneta drošību **inspektoriem, kas strādā pie nepilngadīgo lietām**;

- izstrādāt **spēles bērniem** ("Sivēns lielpilsētā","Sivēna ziemas diena"), kas saistītas ar bērnu drošību internetā un sociālajos tīklos (profila veidošana, fotoattēlu galerija, kā reaģēt uz nezināmu sūtītāju paziņojumiem un negatīviem komentāriem);
- organizēt **seminārus bērniem**; Valsts policija sagatavo materiālus par kiberdrošību dažāda vecuma bērniem, uzsvaru liekot uz briesmām, ar kādām tie var saskarties. Galvenais mērķis ir veidot bērnos izpratni par riskiem, kas saistīti ar šķietami parastām darbībām internetā; materiāli ietver būtiskus padomus par to, ka aizsargāt sevi no kibernoziegumiem. Valsts policija ir arī izstrādājusi brošūru bērniem un pieaugušajiem Braila rakstā;
- publicēt **brošūras vecākiem** par to, kā labāk aizsargāt savus bērnus no seksuālas uzmākšanās tiešsaistē;
- 2015. gadā tika sagatavoti trīs svarīgi **paziņojumi presei**, reaģējot uz kibertelpā izdarītiem dzimumnoziegumiem.

2. Drošāka interneta centra *Net-Safe Latvia* pasākumi

Drošāka interneta centrs *Net-Safe Latvia* (Centrs) ir ES *Safer Internet* programmas *Insafe* tīkla nacionālais kontaktpunkts Latvijā. Projektu līdzfinansēja Eiropas Komisija (50 %). To bija plānots īstenot 18 mēnešos (no 2015. gada 1. janvāra līdz 2016. gada 30. Jūnijam). [14] Centra koordinējošā iestāde ir Latvijas Interneta asociācija sadarbībā ar Valsts bērnu tiesību aizsardzības inspekciju (Inspekcija) un Latvijas Pašvaldību mācību centru. Centra darbs ir koncentrēts uz šādām trim jomām:

- **informēt un izglītot** (mērķa grupas: bērni, pusaudži, skolotāji un vecāki; saturs: interneta satura drošība un iespējamie apdraudējumi (kūdīšana uz naidu, rasisms, bērnu pornogrāfija un pedofīlija, emocionāla vardarbību internetā, identitātes zādzība un datu ļaunprātīga izmantošana));

[14] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka 7.10.2016. tika parakstīta vienošanās par projekta turpināšanu. Jaunais projekts "*SIC Latvia* "*Net-safe II*"" (ko atbalsta Eiropas Komisijas Eiropas infrastruktūras savienošanas instrumenta ietvaros) ilgs no 1.7.2016. līdz 31.8.2018.

- **nodrošināt uzticības tālruni un iespējas sabiedrībai ziņot par nelikumīgu tiešsaistes saturu un pārkāpumiem** (ziņojumi ir anonīmi; tos izskata un vajadzības gadījumā nosūta Valsts policijai turpmākai izmeklēšanai);
- **nodrošināt Inspekcijas uzticības tālruņa 116111 darbību** (lai ikvienam, jo īpaši bērniem un jauniešiem, radītu kādu vietu, kur griezties pēc palīdzības visos ar internetu saistītos jautājumos).

- Triju gadu laikā (2014–2016) uzticības tālrunis ir saņēmis 1968 elektroniski iesniegtus ziņojumus par nelikumīgu tiešsaistes saturu un pārkāpumiem [15].

2015. gadā uzticības tālrunis saņēma zvanus vairāk nekā no 670 bērniem un jauniešiem par jautājumiem, kas saistīti ar internetu (tostarp kiberiebiedēšanu, pornogrāfiju tiešsaistē un bērnu seksuālu izmantošanu), kas ir divas reizes vairāk nekā 2014. gadā. Ir sāktas arī dažādas izglītības iniciatīvas:

- lai izglītotu bērnus un jauniešus jautājumos par interneta drošību, Inspekcija sadarbībā ar Centru ir sagatavojusi videomateriālus, kas atspoguļo trīs situācijas, kādas bērni un jaunieši var piedzīvot vai jau ir piedzīvojuši reālajā dzīve, un ir sagatavojusi arī grāmatu par interneta drošību 5–7 gadus veciem bērniem;
- ir izstrādātas instrukcijas vecākiem par drošu interneta lietošanu;
- personām, kas strādā ar bērniem (skolotājiem, sociālajiem darbiniekiem), ir nodrošināta bezmaksas apmācība.

[15] Turklāt izvērtēšanas grupa tika informēta, ka 2016. gadā Latvijā uz serveriem tika izvietoti 53 ziņojumi, kas saturēja materiālus par bērnu seksuālu izmantošanu; šie ziņojumi tika nosūtīti Valsts policijai izmeklēšanai. 134 ziņojumi, kuri saturēja materiālus par seksuālu vardarbību pret bērniem un kuri netika izvietoti Latvijā, tika iesniegti asociācijas *INHOPE* datubāzei (attiecīgajām valstīm, lai dzēstu šos materiālus no publiskās piekļuves zonas). 2016. gadā, pateicoties labai sadarbībai starp Centru, Valsts policiju un Latvijas interneta pakalpojumu sniedzējiem, visi materiāli par seksuālu vardarbību pret bērniem, kuri bija izvietoti Latvijā un par kuriem bija ziņots Latvijas uzticības tālrunim, tika dzēsti no publiskās piekļuves zonas.

Citi relevanti pasākumi

Lai novērstu bērnu pornogrāfiju un seksuālu izmantošanu internetā, Valsts policija ir izveidojusi videodatni *("police to peer project*"), kas parādīsies automātiski, tiklīdz tiks lejupielādēti attēli vai videodatnes, kas satur bērnu pornogrāfiju un seksuālu izmantošanu. Videodatnē policijas darbinieks informē ļaunprātīgo izmantotāju, ka policija ir noskaidrojusi viņa vai viņas IP adresi un ka ir sākts identifikācijas process, un sniedz informāciju par kriminālapsūdzībām.

6.2.4. Dalībnieki un pasākumi cīņā pret tīmekļa vietnēm, kas satur vai izplata bērnu pornogrāfiju

Saskaņā ar Kriminālprocesa likuma 239. panta ceturto daļu notikuma vietas apskates laikā operācijas veicējs var izņemt priekšmetus ar noziedzīga nodarījuma pēdām (tostarp nodarījumi, kas saistīti ar seksuālu vardarbību pret bērniem tiešsaistē un bērnu pornogrāfiju).

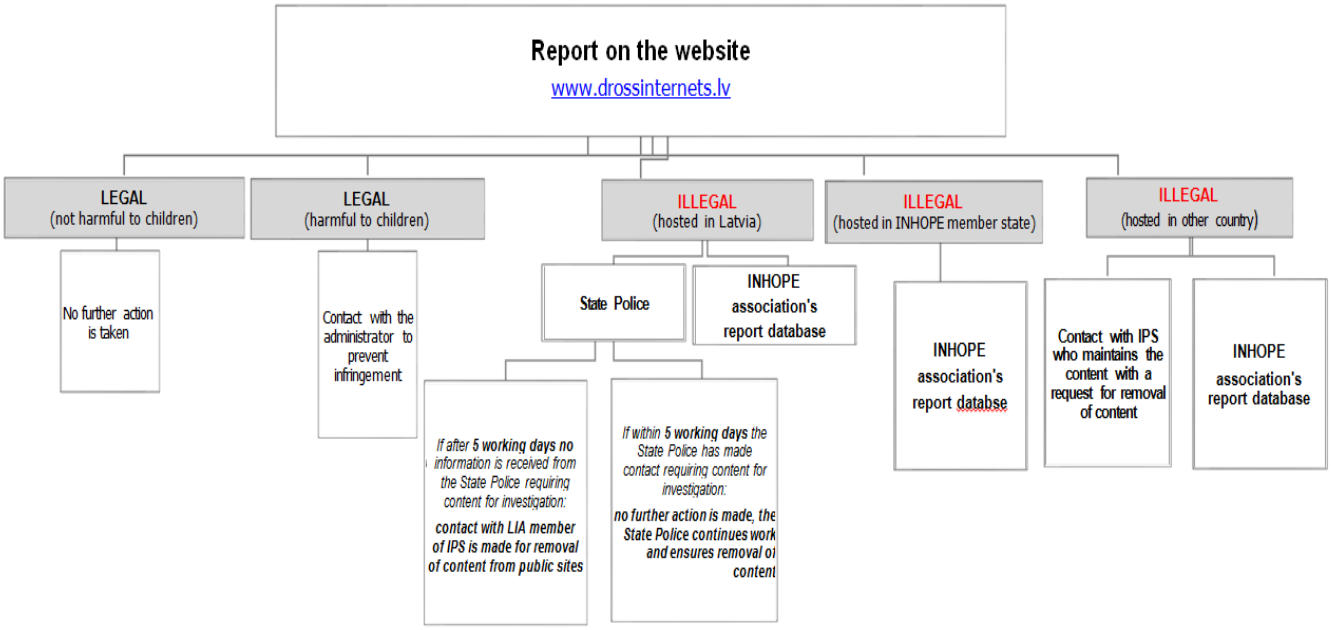
Nav nekādu tehnisku līdzekļu, ar ko filtrēt tīmekļa vietnes, kurās ir bērnu pornogrāfijas materiāli. Tomēr Valsts policija šajā sakarā sadarbojas ar Centru. Amatpersona, kas ir pilnvarota veikt kriminālprocesu, var arī pilnvarot izņemt tīmekļa lapas saturu. [16]

Elektronisko sakaru pakalpojumu sniedzējiem nav juridiska pienākuma *ex officio* bloķēt piekļuvi, izņemt saturu vai likvidēt tīmekļa lapas. Tomēr daži pakalpojumu sniedzēji (piemēram, valsts sociālo plašsaziņas līdzekļu platforma www.draugiem.lv) sadarbojas ar tiesībaizsardzības iestādēm uz brīvprātības pamata (ziņojot par nelikumīgu saturu, ko tie identificējuši un bloķējuši vai izņēmuši).

[16] Pēc apmeklējuma izvērtēšanas grupa tika informēta, ka Valsts policija ir radījusi tehniskus līdzekļus, ar ko filtrēt tīmekļa vietnes, kurās ir bērnu pornogrāfijas materiāli. Minētie līdzekļi šobrīd tiek testēti.

Turklāt Centrs – kā *INHOPE* loceklis°– apstrādā saņemtos ziņojumus un vajadzības gadījumā nosūta tos Valsts policijai turpmākai izmeklēšanai.

Skatīt turpmāk attēloto diagrammu ar informāciju par Centra un Valsts policijas sadarbību:



Kriminālprocesa likums ietver sevī vienlīdzības principu, ar kuru tiek atbalstīta vienota procesuālā kārtība visām kriminālprocesā iesaistītajām personām. Tāpēc nav ieviesta nekāda atsevišķa procedūra steidzamiem gadījumiem. Tomēr Bērnu tiesību aizsardzības likumā ir noteikts, ka tiesiskās attiecībās, kas skar bērnu, bērna tiesības un intereses ir prioritāras.

Gadījumi, kad serveris atrodas ārpus Latvijas teritorijas, tiek risināti saskaņā ar Konvenciju par kibernoziegumiem un izmantojot Interpola un Eiropola informācijas kanālus.

Nav nevienas specializētas struktūrvienības, kas nodarbotos tikai ar bērnu pornogrāfijas gadījumiem.

6.3. Krāpnieciski darījumi ar norēķinu kartēm tiešsaistē

6.3.1. Ziņošana tiešsaistē

Ir ieviests pienākums ziņot Valsts policijai par visiem krāpnieciskiem nodarījumiem ar norēķinu kartēm. Ziņojumi lielākoties tiek iesniegti, izmantojot vispārējo tālruņa numuru, vai nosūtīti pa e-pastu uz kanc@vp.gov.lv. Tomēr praksē komercbankas bieži vien neziņo tiesībaizsardzības iestādēm par nodarījumiem, jo pastāv risks, ka tās var zaudēt savu klientu uzticību.

6.3.2. Privātā sektora loma

Latvijas iestādes uzskata, ka sadarbība ar privāto sektoru ir efektīva. Piemēram, Valsts policija (Ekonomisko noziegumu apkarošanas pārvaldes Kibernoziegumu apkarošanas nodaļa) uztur regulāru dialogu ar Latvijas Komercbanku asociāciju (kura uz brīvprātības pamata apvieno Latvijā reģistrētas bankas un ārvalstu banku filiāles) un aktīvi piedalās trīspusējās sadarbības platformā kopā ar banku drošības struktūrvienībām un CERT.LV.

Praksē komercbankas Latvijā periodiski maina bankomātu komponentus, lai ierobežotu datu pārkopēšanas iespējas. Šī procedūra ir ieviesta arī automātiskas apkalpošanas (degvielas uzpildes) stacijās. Turklāt vairākas komercbankas ir veikušas papildu pasākumus, lai nodrošinātu tiešsaistes maksājumu drošību. Turklāt, lai brīdinātu un aizsargātu potenciāli cietušās personas, policija un komercbankas regulāri sniedz sabiedrībai informāciju par kibernoziedzības riskiem un par to, kā aizsargāt personas datus.

6.4. Secinājumi

- Ir ieviests reaģēšanas mehānisms, lai cīnītos pret kiberuzbrukumiem. Valstij radītu draudu gadījumā Ministru kabinets var nolemt nodot CERT.LV uzdevumus, tiesības un resursus Nacionālajiem bruņotajiem spēkiem. Mazāk bīstamos gadījumos CERT.LV ziņo Aizsardzības ministrijai, kura pēc tam konsultējas ar Nacionālo IT drošības padomi un ziņo Ministru kabinetam, ja ir pieņemti vajadzīgie lēmumi. Latvijā ir ieviesti kritiskajai IT infrastruktūrai paredzēti īpaši tiesību akti. CERT.LV organizē mācības reaģēšanai uz incidentiem, kuras paredzētas IT ekspertiem ne tikai tehniskā līmenī, bet arī vadības līmenī.

- CERT.LV ir svarīga nozīme kiberdrošības struktūrā, un tā darbojas kā starpnieks starp privāto sektoru, akadēmiķiem un policiju. Tā ir labi nokomplektēts un prasmīgs partneris, kas sniedz atbalstu publiskajām iestādēm un sabiedrībai kopumā. Tā ļoti aktīvi piedalās publiskajās debatēs par kiberdrošību. Tā arī risina lielāko daļu drošības incidentu jautājumu, un tā ir noslēgusi vienošanās ar visiem nozīmīgākajiem elektronisko sakaru pakalpojumu sniedzējiem, lai ātri un efektīvi informētu cietušos (to atbalsta CERT.LV zvanu centrs).

- Vienošanās ar CERT.LV par plašāku brīvprātīgu ziņošanu un brīvprātīgu sadarbību ar citiem sektoriem, tādiem kā banku sektors, pastiprina galveno dalībnieku, piemēram, valsts iestāžu, valsts kritiskās infrastruktūras apsaimniekotāju un interneta pakalpojumu sniedzēju, pienākumu ziņot par nozīmīgiem kiberdrošības incidentiem, pamatojoties uz IT drošības likumu. Tādējādi Latvija lielā mērā spēj neitralizēt nepietiekamu ziņošanu, kas saistīta ar bailēm kaitēt reputācijai, un spēj nodrošināt samērā visaptverošu statistiku par kiberdrošības incidentu skaitu.

- Pieminēšanas vērta ir arī Latvijas ciešā sadarbība ar kaimiņvalstīm. 2015. gada novembrī tika parakstīts saprašanās memorands starp visu triju Baltijas valstu *CERT* vienībām, apņemoties pastiprināt sadarbību kiberdrošības un IT sistēmu un tīklu aizsardzības jomā.

- Īpaši jāpiemin Kiberaizsardzības vienība – jaunizveidota brīvprātīga struktūra, kas sniedz atbalstu Nacionālajiem bruņotajiem spēkiem, reaģējot uz IT drošības incidentiem un mazinot to sekas. Tā cieši sadarbojas ar Aizsardzības ministriju un ar CERT.LV. Tā nodrošina ļoti inovatīvu pieeju speciālo zināšanu apmaiņai starp privāto un publisko sektoru, jo brīvprātīgie no privātā sektora nāk ar zināšanām un pieredzi, sadarbojas un apmainās ar šo pieredzi ar saviem kolēģiem publiskajā sektorā. Tā kā šāda dalība ir brīvprātīga, izmaksu un resursu ieguldījumu atdeve ir ļoti pozitīva publiskajām iestādēm. Brīvprātīgie ar savām jaunas apmācības spējām palīdz veidot drošu kibertelpu Latvijā un arī nodrošina resursu kopumu, ko vajadzības gadījumā var izmantot kopā ar publisko struktūru minimālu ieguldījumu.

- Kibernoziedzības prevencijā svarīga nozīme ir arī nevalstiskajām organizācijām, tādām kā Digitālās drošības alianse un *Net-Safe*, ar kurām izvērtēšanas grupa tikās apmeklējuma laikā. Šīs organizācijas ir ļoti aktīvas kibernoziedzības prevencijas jomā un aktīvi sadarbojas ar skartajiem rūpniecības sektoriem un neaizsargātām grupām. *Net-Safe* nozīme – jo īpaši kibernoziedzības prevencijā un atbalsta sniegšanā seksuālas vardarbības pret bērniem tiešsaistē un pornogrāfijas gadījumos – būtu izceļama kā paraugprakses piemērs.

- Tika skarti daži jautājumi, kurus izvirzīja jo īpaši privāto organizāciju asociācijas, tostarp bankas, par personas datu izmānīšanas jeb pikšķerēšanas incidentu un/vai nelielu kibernoziedzības incidentu pārvarēšanu. Atkārtoti kā problēma tika minēts tas, ka kriminālizmeklēšanu nevar sākt, ja nav iespējams skaidri konstatēt pietiekamu kaitējumu, – pat tad, kad ir skaidrs, ka tiek veikta nelikumīga darbība. Tas daudzus attur no ziņošanas par kibernoziegumu mēģinājumiem, piemēram, pikšķerēšanu, kuri – ja vien tie nav sekmīgi – nebeidzas ar kaitējuma radīšanu cietušajiem. Pat tad, ja var konstatēt zaudējumus, tie netiek uzskatīti par pietiekamiem, lai par iespējamo noziegumu ziņotu kompetentajām iestādēm. Tas neļauj savlaicīgi atklāt šādus kibernoziegumu veidus un ļauj tiem turpināties līdz brīdim, kad ir kāds cietušais, kam ir nodarīts nopietns kaitējums.

- Šķiet, ka dažādu struktūru izpratne par sekmīgu sadarbību starp privāto un publisko sektoru atšķiras. Publiskās iestādes esošo sadarbību uzskata par izcilu un pietiekamu, kurpretim asociācijas to raksturo mazāk pozitīvi. Privātās struktūras vēl arvien ļoti atzinīgi vērtē esošās sadarbības vietas un kanālus, tomēr tās noteikti vēlētos papildu pasākumus, lai atvieglotu krimināvajāšanu par kibernoziegumiem un padarītu to izmaksu ziņā lētāku cietušajiem. Šķiet, ka pastāv iespēja stiprināt sadarbību starp privāto un publisko sektoru, piemēram, ar finanšu sektoru valsts līmenī.

- Turklāt šķiet, ka privātās struktūras bieži vien nedalās ar informāciju par kiberuzbrukumiem ne ar Valsts policiju, ne arī pašas savā starpā. Tas savukārt neļauj sekmīgi novērst, konstatēt, izmeklēt kibernoziegumus un veikt krimināvajāšanu par tiem. Tāpēc izvērtētāji uzskata, ka Latvijai būtu jāapsver iespēja ieviest juridisku pienākumu ziņot par kiberuzbrukumiem visvairāk skartajiem un neaizsargātākajiem sektoriem, tādiem kā banku sektors, interneta pakalpojumu sniedzēji un ar liela personas datu apjoma apstrādi saistītie pakalpojumi, – pat tad, ja tie nav kritiskās infrastruktūras daļa.

7. STARPTAUTISKĀ SADARBĪBA

7.1. Sadarbība ar ES aģentūrām

*7.1.1. Formālās prasības sadarbībai ar Eiropolu/*EC3*,* Eurojust *un* ENISA

Nav nekādu formālu prasību sadarbībai starp Latvijas iestādēm un Eiropolu/*EC3*, *Eurojust* un *ENISA* attiecībā uz kibernoziedzības gadījumiem.

*7.1.2. Novērtējums par sadarbību ar Eiropolu/*EC3*,* Eurojust *un* ENISA

EIROPOLS/*EC3*

To gadījumu skaits, kuros Latvijai būtu vajadzīga Eiropola/*EC3* palīdzība, ir neliels. Tomēr šo gadījumu skaits pieaug. Valsts policija 2015. gadā saņēma un apstrādāja 54 (Eiropola/*EC3* sūtītos) pieprasījumus. Turklāt Latvija ir apliecinājusi savu gatavību turpināt sniegt citām ES dalībvalstīm un attiecīgajām trešām valstīm vajadzīgo palīdzību.

- Latvija augstu vērtē to, ka ES politikas cikls organizētas un smagas starptautiskas noziedzības jomā un operatīvie rīcības plāni tiek īstenoti kā prioritāte kibernoziedzības apkarošanā. Latvija piedalās visās apakšprioritātēs.
- Tā arī skaidri saskata pievienoto vērtību, kas piemīt kontaktpunktiem (*Terminal*, *Cyborg* un citiem), Kopīgajai kibernoziedzības rīcības uzdevumgrupai (*J-CAT*) un Eiropola ekspertu platformai (kura ir vērtīgs avots/līdzeklis papildu zināšanu un informācijas iegūšanai par jaunākajām kibernoziedzības tendencēm).

Turklāt vienam Valsts policijas ekspertam ir deleģēts uzdevums piedalīties *EC3* platformas darbā, kuras mērķis ir analizēt ļaunprogrammatūras (Eiropas ļaunprogrammatūru analīzes risinājums, ar kuru atbalsta tiesu ekspertīzi attiecībā uz ļaunprogrammatūras darbību izmēģināšanas vidē). Latvija uzskata to par svarīgu ieguldījumu Valsts policijas ekspertīžu un izmeklēšanas spēju veidošanā.

Latvijai ir laba pieredze sadarbībā ar Eiropolu un Interpolu konkrētos gadījumos, piemēram, izmantojot operatīvo sanāksmi Eiropolā par Latvijā izveidotu noziedzīgu grupu, kas organizēja bankomātu skimerus Baltijā, Apvienotajā Karalistē, Polijā un Krievijā. Tā rezultātā Zviedrijā un Krievijā tika aizturēti vairāki šīs noziedzīgās grupas locekļi.

Latvija piedalās Eiropolā izveidotajā Eiropas Savienības stratēģiskajā grupā, kas pulcē augsto tehnoloģiju noziegumu izmeklēšanas valstu vienību vadītājus (Grupa), bet ierobežoto cilvēkresursu dēļ 2015. gadā tā nevarēja apmeklēt Grupas sanāksmes.

Turklāt 2014. gadā Valsts policija piedalījās starptautiskajā operācijā *HAVEN* (*Halting Europeans Abusing Victims in Every Nation*), kuras mērķis ir atbalstīt ES dalībvalstis, palīdzot tām atklāt un aizturēt bērnu seksuālus izmantotājus, kas ceļo nolūkā ļaunprātīgi izmantot bērnus.

Eurojust

Ģenerālprokuratūra jo īpaši augstu vērtē *Eurojust* sniegto palīdzību (it sevišķi attiecībā uz lūgumu par tiesisko palīdzību sarežģītās lietās savlaicīgāku izpildi). Latvijas iestādes uzsvēra koordinācijas sanāksmju pievienoto vērtību, jo tās ir instruments, ar ko veicina efektīvāku izmeklēšanu un pierādījumu vākšanu. 2014. un 2015. gadā Ģenerālprokuratūra neiesniedza *Eurojust* nevienu lūgumu par palīdzību kibernoziedzības lietās.

Valsts policija piedalījās *Eurojust* taktiskajās sanāksmēs par kibernoziedzības teritoriālo jurisdikciju un jautājumiem, kas saistīti ar pierādījumiem. Šī pieredze tiek uzskatīta par profesionāli noderīgu.

ENISA

ENISA ir noderīga informācijas apmaiņas vieta; tāpat Latvija augstu vērtē tās analītiskos dokumentus un pētniecību.

7.1.3. Kopējo izmeklēšanas grupu un kiberpatruļu darbības rezultāti

Latvija vēl nav piedalījusies nevienā kopējā izmeklēšanas grupā saistībā ar kibernoziegumiem. Tomēr Latvijas iestādes uzskata, ka tādi instrumenti kā kopējas izmeklēšanas grupas un kiberpatruļas ir vērtīgi sadarbības instrumenti un ka tie ir jāizmanto vairāk.

7.2. Sadarbība starp Latvijas iestādēm un Interpolu

Latvijas iestāžu iesaiste sadarbībā ar Interpolu kibernoziedzības gadījumos ir mazāk regulāra nekā ar Eiropolu/*EC3*. Valsts policija saņem Interpola Kibernoziedzības datu apkopošanas centra (*Cyber Fusion Centre*) darbības pārskatus, kuri nenoliedzami sekmē tās kopējo darbu. Apmeklējuma laikā tika plānots līdz 2016. gada 30. jūnijam nodrošināt piekļuvi Starptautiskajai Bērnu seksuālas izmantošanas (*ICSE*) datubāzei (ar plānotajiem diviem savienojuma punktiem un sešām amatpersonām paredzēto apmācību).

7.3. Sadarbība ar trešām valstīm

Nosūtot tiesiskās palīdzības lūgumus Latvijai, trešās valstis bieži izmanto Eiropolu kā kanālu. Latvija augstu vērtē Eiropola koordinējošo lomu šajā jomā. Budapeštas Konvencija, Eiropas Konvencija par savstarpējo palīdzību krimināllietās un divpusējie nolīgumi nodrošina juridisko pamatu.

Sadarbība ar ASV balstās uz Līgumu starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību. To piemēroja Latvijas pilsoņa izdošanai, kurš apsūdzēts kibernoziegumos.

7.4. Sadarbība ar privāto sektoru

Kad (uzņēmumu, kuru galvenā mītne atrodas trešā valstī) vietējās filiāles tiek reģistrētas Latvijā (Uzņēmumu reģistrā vai Komercreģistrā), tiek veikta informācijas apmaiņa un/vai procesuālas darbības (tostarp piespiedu pasākumi) saskaņā ar valsts tiesību aktiem.

Pirms pirmstiesas izmeklēšanas tiek izmantoti Eiropola, Interpola un policijas sadarbības informācijas sakaru kanāli. Pirmstiesas izmeklēšanas laikā tiek pētīti attiecīgie savstarpējas tiesiskās palīdzības instrumenti un Eiropola un *Eurojust*, tostarp kopējo izmeklēšanas grupu, sniegtās iespējas.

7.5. Starptautiskās sadarbības instrumenti

7.5.1. Savstarpēja tiesiskā palīdzība

Latvijā nav konkrēta juridiskā pamata savstarpējas tiesiskās palīdzības sniegšanai kibernoziegumu jomā. Šajā jomā piemēro Kriminālprocesa likumā (C daļa "Starptautiskā sadarbība krimināltiesiskajā jomā") un divpusējos nolīgumos izklāstītos noteikumus. Saskaņā ar Kriminālprocesa likumu (846. pants par kompetentajām iestādēm ārvalsts lūguma izskatīšanā):

- *pirmstiesas procesā*: ārvalstu lūgumus izskata un izlemj Ģenerālprokuratūra, bet līdz kriminālvajāšanas uzsākšanai to var darīt arī Valsts policija;
- *pēc lietas nodošanas tiesai*: ārvalstu lūgumus izskata un izlemj Tieslietu ministrija.

I. Statistika par saņemto lūgumu skaitu

Ģenerālprokuratūra:

Gads	Kibernoziegumi	Bērnu pornogrāfija un seksuāla izmantošana	Nelikumīgas darbības ar finanšu instrumentiem un maksāšanas līdzekļiem
2014	102	4	2
2015	75	1	3

Sadarbības juridiskie pamati

— Protokols, kas pievienots Konvencijai par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās, ko Padome izstrādājusi saskaņā ar Līguma par Eiropas Savienību 34. pantu (157);

— Eiropas Savienības Konvencija par savstarpēju palīdzību krimināllietās (5, Turcija, Šveice);

— Līgums starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību (20);

— Līgums starp Latvijas Republiku un Baltkrievijas Republiku par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (3);

— Līgums starp Latvijas Republiku un Moldovas Republiku par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (1);

— Līgums starp Latvijas Republiku un Krievijas Federāciju par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (1).

Valsts policija:

Gads	Kibernoziegumi	Bērnu pornogrāfija un seksuāla izmantošana	Nelikumīgas darbības ar finanšu instrumentiem un maksāšanas līdzekļiem
2014	9	2	175
2015	7	1	218

Sadarbības juridiskie pamati

— Eiropas Konvencija par savstarpējo palīdzību krimināllietās (Albānija – 1, Horvātija – 1; Gruzija – 1, Islande – 1, Lihtenšteina – 4, Norvēģija – 1, Šveice – 3, Turcija – 3);

— Protokols, kas pievienots Konvencijai par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās, ko Padome izstrādājusi saskaņā ar Līguma par Eiropas Savienību 34. pantu;

— Līgums starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību (19);

— Līgums starp Latvijas Republiku un Baltkrievijas Republiku par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (3);

— Līgums par tiesisko palīdzību starp Latvijas Republiku, Igaunijas Republiku un Lietuvas Republiku (Lietuva – 58, Igaunija – 6);

— Līgums starp Latvijas Republiku un Polijas Republiku par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes, darba un krimināllietās (97);

— Līgums starp Latvijas Republiku un Krievijas Federāciju par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (10);

— Līgums starp Latvijas Republiku un Uzbekistānas Republiku par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes, darba un krimināllietās (1).

II. Statistika par nosūtīto lūgumu skaitu

Ģenerālprokuratūra:

Krimināllikums					
Gads	**243. pants**	**162. pants**	**166. pants**	**177.[1] pants**	**193.[1] pants**
2014	1	0	0	1	0
2015	0	1	2	4	7

Sadarbības juridiskie pamati

— Līgums starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību (5);

— Līgums starp Latvijas Republiku un Krievijas Federāciju par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (8);

— Protokols, kas pievienots Konvencijai par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās, ko Padome izstrādājusi saskaņā ar Līguma par Eiropas Savienību 34. pantu (2), savstarpējas atzīšanas princips (1 – Apvienotie Arābu Emirāti).

Valsts policija:

Krimināllikums								
Gads	**144. pants**	**166. pants**	**177.[1] pants**	**193.[1] pants**	**241. pants**	**243. pants**	**244. pants**	**244.[1] pants**
2014	5	1	1	13	0	1	0	0
2015	4	2	4	33	1	0	1	3

Sadarbības juridiskie pamati

— Eiropas Konvencija par savstarpējo palīdzību krimināllietās (Apvienotie Arābu Emirāti – 1, Šveice – 2);

— Protokols, kas pievienots Konvencijai par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās, ko Padome izstrādājusi saskaņā ar Līguma par Eiropas Savienību 34. pantu;

— Līgums starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību (12);

— Līgums par tiesisko palīdzību starp Latvijas Republiku, Igaunijas Republiku un Lietuvas Republiku (Lietuva – 5, Igaunija – 1);

— Līgums starp Latvijas Republiku un Krievijas Federāciju par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes un krimināllietās (7);

— Līgums starp Latvijas Republiku un Ukrainu par tiesisko palīdzību un tiesiskajām attiecībām civilajās, ģimenes, darba un krimināllietās (1).

Tiesas procesa stadijā nav lūgta vai saņemta nekāda tiesiskā palīdzība attiecībā uz kibernoziegumiem. Nav nekādu īpašu procedūru vai nosacījumu, kas būtu jāievēro, lai nosūtītu savstarpējas tiesiskās palīdzības lūgumu. Vidējais atbildes sniegšanas termiņš ir divi mēneši; tomēr steidzami lūgumi tiek izskatīti pēc iespējas drīz (tas neattiecas uz tiesas procesa stadiju, jo nav lūgta nekāda tiesiskā palīdzība).

Tā kā savstarpēja tiesiskā palīdzība attiecībā uz kibernoziegumiem netiek nošķirta no citiem noziedzīgiem nodarījumiem, Latvija nodrošina sadarbību saskaņā ar Kriminālprocesa likumu. Var pieprasīt šādas darbības: personas izdošanu kriminālvajāšanai, tiesāšanai vai sprieduma izpildei vai medicīniska rakstura piespiedu līdzekļu noteikšanai; kriminālprocesa nodošanu; procesuālo darbību izpildi; ar brīvības atņemšanu nesaistīta drošības līdzekļa izpildi; sprieduma atzīšanu un izpildi; un citas starptautiskajos līgumos paredzētas darbības. Visizplatītākie savstarpējas tiesiskās palīdzības lūgumu iemesli ir informācijas pieprasījumi no elektronisko sakaru komersantiem un kredītiestādēm, lai palīdzētu tiem labāk sagatavoties nopratināšanai.

Tiek izmantoti lūgumi par tiesisko palīdzību kriminālllietās par kibernoziegumiem. Tomēr Latvijas iestādes norāda, ka šis process ir pārāk garš un diezgan apgrūtinošs. Latvija pauda viedokli, ka savstarpējas tiesiskās palīdzības instrumenti kā tādi nav paredzēti, lai apmierinātu digitālā laikmeta vajadzības.

7.5.2. Savstarpējas atzīšanas instrumenti

Pēdējo divu gadu laikā Ģenerālprokuratūra ir izpildījusi īpašuma vai pierādījumu iesaldēšanas rīkojumus trīs reizes. Citi ES savstarpējas atzīšanas instrumenti nav izmantoti.

7.5.3. Nodošana/izdošana

Izdošanas procedūras Latvijā reglamentē Kriminālprocesa likuma 65. nodaļa par personas izdošanu Latvijai un 66. nodaļa par personas izdošanu ārvalstij. Tādējādi visi Krimināllikumā paredzētie kibernoziedzības nodarījumi ietilpst Eiropas apcietināšanas ordera darbības jomā; tie var būt iemesls nodošanai, un to dēļ var piemērot izdošanu (jo tie atbilst Kriminālprocesa likuma 682. panta un 696. panta prasībām).

Saskaņā ar Kriminālprocesa likumu (65. un 66. nodaļa) Ģenerālprokuratūra ir iestāde, kas ir atbildīga par izdošanas un nodošanas jautājumiem. Tiek izmantoti tiešie kanāli, diplomātiskie kanāli, Interpola sakaru kanāli un Šengenas informācijas sistēma.

I. Statistika par saņemto izdošanas lūgumu skaitu

Gads	Datornoziegumi	Bērnu pornogrāfija un seksuāla izmantošana	Nelikumīgas darbības ar finanšu instrumentiem un maksāšanas līdzekļiem
2014	1	0	0
2015	7	0	0

Padomes Pamatlēmums (2002. gada 13. jūnijs) par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm.

II. Statistika par nosūtīto izdošanas lūgumu skaitu

Gads	Krimināllikums 162. pants	Krimināllikums 166. pants	Krimināllikums 193.[1] pants
2014	5	0	1
2015	1	1	2

2012. gada 2. decembrī Amerikas Savienotās Valstis saskaņā ar Līgumu starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību iesniedza Ģenerālprokuratūrai lūgumu par kāda kibernoziegumos apsūdzēta Latvijas pilsoņa izdošanu. 2012. gada 23. augustā ASV Ņujorkas Dienvidu rajona apgabaltiesa apsūdzēja Latvijas pilsoni par iesaistīšanos shēmā nolūkā izplatīt datorvīrusu, kas inficēja vairāk nekā vienu miljonu datoru visā pasaulē un radīja desmitiem miljonu dolāru lielus zaudējumus. 2012. gada 2. decembrī ASV saskaņā ar Līgumu starp Latvijas Republikas valdību un Amerikas Savienoto Valstu valdību par savstarpējo tiesisko palīdzību iesniedza Ģenerālprokuratūrai izdošanas lūgumu. 2012. gada 6. decembrī Rīgas pilsētas Centra rajona tiesa izdeva rīkojumu par izdošanas apcietinājumu. 2012. gada 20. decembrī Ģenerālprokuratūra pieņēma lēmumu par to, ka pamats izdošanai ir pieņemams; 2013. gada 31. janvārī Latvijas Republikas Augstākā tiesa apstiprināja tās lēmumu. 2013. gada 12. aprīlī Latvijas Republikas tiesībsargs nosūtīja lūgumu ministru prezidentam, lūdzot izvērtēt iespējamos Eiropas Cilvēktiesību konvencijas (Konvencija) pārkāpumus un iegūt informāciju par cilvēktiesību garantijām Amerikas Savienotajās Valstīs, lai novērstu iespējamos cilvēktiesību pārkāpumus. 2013. gada 4. jūlijā ASV vēstniecība Latvijā atbildēja, ka Latvijas pilsoņa izdošanas ASV gadījumā tiks nodrošinātas vispārējās cilvēktiesības (tostarp, piemēram, tiesības uz juridisko palīdzību un advokātu). 2013. gada 31. maijā Latvijas Republikas Satversmes tiesa pieņēma nolēmumu, ka nav nekādu cilvēktiesību pārkāpumu izdošanas gadījumā. 2015. gada 9. februārī Latvijas pilsonis tika izdots ASV. 2015. gada 5. septembrī Latvijas pilsonis atzina sevi par vainīgu, un viņu sodīja ar brīvības atņemšanu uz laiku, kas līdzvērtīgs laikam, kuru viņš jau pavadījis apcietinājumā.

7.6. Secinājumi

- Praktiķi, kas piedalās kibernoziegumu izmeklēšanā un kriminālvajāšanā par tiem, pazīst Eiropolu un *Eurojust*. Visas attiecīgās valsts iestādes uzskata, ka sadarbība ar šīm ES aģentūrām ir apmierinoša. Tā kā kriminālizmeklēšanu kibernoziedzības jomā galvenokārt veic Valsts policija, tā ir Valsts policija, kas izmanto šo ES struktūru piedāvātās sadarbības iespējas.

- Valsts policija atzinīgi vērtēja *Eurojust* organizētās tematiskās sanāksmes, kas ļauj apmainīties ar pieredzi par izmeklēšanas metodēm un instrumentiem tiesu iestāžu sadarbībai ar ES dalībvalstu praktiķiem. Kibernoziegumu izmeklēšanā Valsts policija ir plaši un sekmīgi izmantojusi sadarbību ar Eiropolu/*EC3* un uzskata to par ļoti lietderīgu. Tomēr tiekoties praktiķi minēja, ka tie ļoti vēlētos, lai tiktu izveidots forums, kur var regulārāk apmainīties ar pieredzi starp ES dalībvalstu kompetentajām iestādēm jautājumā par kriminālvajāšanu kibernoziedzības lietās.

- Tiekoties praktiķi minēja, ka ES līmenī ir jānosaka efektīvs veids, kā paziņot par savstarpējas tiesiskās palīdzības lūgumiem, ko ES dalībvalstis nosūta nozīmīgākajiem interneta pakalpojumu sniedzējiem, kas atrodas ārpus ES, un kā izpildīt šādus lūgumus. Sistēma šādu lūgumu nosūtīšanai tieši attiecīgajiem ārpussavienības interneta pakalpojumu sniedzējiem saskaņā ar saskaņotu nosacījumu kopumu ievērojami uzlabotu sadarbību. Būtu arī vēlams, lai ES aģentūras varētu sniegt informāciju par iespējām sadarbībai ar trešām valstīm un ar šo sadarbību saistītajām prasībām un pieredzi.

- Latvijas praktiķi izmanto visus pieejamos kanālus, lai sniegtu tiesisko palīdzību: divpusējas attiecības, sadarbības koordinatorus, tiesnešus koordinatorus un ES aģentūras. Tika uzsvērts, ka sadarbība, kas iespējama saskaņā ar esošajiem tiesiskās palīdzības instrumentiem, bieži vien ir pārāk lēna, lai cīnītos pret tādiem kibernoziegumu veidiem, saistībā ar kuriem elektronisku pierādījumu ātra nodrošināšana ir īpaši svarīga. Bez ātras rīcības – dienas vai divu dienu laikā pēc nozieguma izdarīšanas – bieži vien nav iespējams nodrošināt pietiekamus pierādījumus sekmīgai izmeklēšanai un kriminālvajāšanai. Pašreiz pieejamo tiesu iestāžu sadarbības instrumentu lēna izpilde tika minēta kā viens no galvenajiem šķēršļiem sekmīgai kriminālvajāšanai. Tāpēc izvērtētāji uzskata, ka ES būtu jāapsver, kā tā varētu palīdzēt paātrināt tiesiskās un tiesu iestāžu sadarbības procedūras starp ES dalībvalstīm un trešām valstīm.

8. APMĀCĪBA, INFORMĒTĪBAS VEICINĀŠANA UN PREVENCIJA

8.1. Specializēta apmācība

Tiesu iestādes

Latvijas Tiesnešu mācību centrs nodrošina tālākizglītību tiesnešiem un tiesu darbiniekiem. Ir veikti vairāki dažādi profesionālās kvalifikācijas veidošanas pasākumi (semināri, pieredzes apmaiņas braucieni utt.), īpašu uzmanību pievēršot tiesas spriedumu kvalitātes jautājumiem un uzlabojumiem, kā arī darba kvalitātei ES juridiskajā sistēmā.

Tāpat Latvijas Tiesnešu mācību centrs nodrošina apmācību citiem praktizējošiem juristiem, tostarp prokuroriem, advokātiem, juristiem un valsts struktūru un pašvaldības iestāžu darbiniekiem.

2015. gadā 32 tiesneši un 19 tiesnešu palīgi apmeklēja mācību kursus "Kibernoziedzība I" un "Kibernoziedzība II" (90 minūtes katrs) un divi tiesneši piedalījās divu dienu seminārā "Elektronisko pierādījumu meklēšanas un izņemšanas plānošana un pamatojums: praktiskie jautājumi praktizējošiem juristiem kriminālprocesos pirms pierādījumu iesniegšanas tiesā" (ko Rīgā organizēja Eiropas tiesību akadēmija).

Tiesnešu kvalifikācijas kolēģija reizi piecos gados (pēc tiesneša apstiprināšanas amatā uz neierobežotu laiku) izvērtē tiesneša profesionālo darbu. Izvērtēšanas procesā Tiesnešu kvalifikācijas kolēģijai ir arī pienākums analizēt tiesnešu dalību pasākumos, kuru mērķis ir uzlabot viņu kvalifikāciju. Daži mācību kursi ir pieejami arī tiešsaistē.

Tiesībaizsardzība

Tiesībaizsardzības iestāžu personāla apmācību nodrošina Valsts policijas koledža, kas ir Valsts policijas pārziņā esoša mācību iestāde. Tā nodrošina profesionālo apmācību un tālākizglītību Valsts policijas personālam. Attiecībā uz tālākizglītību 2015. gadā:

- 133 amatpersonas/policijas darbinieki piedalījās ikdienējas mācīšanās programmā "Jaunāko IT izmantošana policijas darbā" (astoņas akadēmiskās stundas), kas turpinās 2016. gadā;
- 65 amatpersonas/policijas darbinieki piedalījās programmā "Elektronisko sakaru metodes internetā: to veidi, lietojums un kontroles līdzekļi" (astoņas akadēmiskās stundas);
- 42 amatpersonas/policijas darbinieki piedalījās programmā "Elektronisko sakaru komersantu datu izmantošana noziedzīgu nodarījumu izmeklēšanā" (astoņas akadēmiskās stundas).

Papildus ir ieviesta profesionālās attīstības programma "IT izmantošana cīņā pret noziedzību", kas aptver šādas specialitātes:

- IT speciālists (120 akadēmiskās stundas);
- informācijas apstrādes un analīzes speciālists (120 akadēmiskās stundas);
- IT speciālists cīņā pret kibernoziedzību (120 akadēmiskās stundas).

Turklāt, kas attiecas uz apmācību un zināšanu apmaiņu, Valsts policija (Ekonomisko noziegumu apkarošanas pārvaldes Kibernoziegumu apkarošanas nodaļa) ikdienā sadarbojas ar dažādiem Latvijas IT uzņēmumiem un programmatūru ražotājiem.

Valsts policijas darbinieki (infotehnisko ekspertīžu speciālisti un kibernoziegumu izmeklētāji) piedalās tālākizglītībā, ko nodrošina Valsts policijas koledža, kā arī mācību kursos, ko nodrošina *CEPOL*, Eiropols un citas struktūras.

CEPOL

Valsts policijas darbinieki bieži piedalās *CEPOL* apmācībā.

2014. gadā septiņi Valsts policijas darbinieki piedalījās mācību kursos par kibernoziedzību un deviņi darbinieki piedalījās kursos tiešsaistē. 2015. gadā septiņi Valsts policijas darbinieki piedalījās mācību kursos par kibernoziedzību un trīs darbinieki piedalījās kursos tiešsaistē.

2015. gada martā ES Padomes prezidentvalsts Latvija sadarbībā ar *CEPOL* organizēja konferenci "Kibernoziedzība – stratēģiskais līmenis", kas bija vērsta uz sadarbības metožu uzlabošanu un izmeklēšanas metožu saskaņošanu pārrobežu gadījumos, kas saistīti ar kibernoziedzību; apdraudējumu un risku identificēšanu kibernoziedzībā; paraugprakses apmaiņu kibernoziegumu izmeklēšanā; redzējuma izstrādi policijas turpmākai sadarbībai kibernoziedzības apkarošanas nolūkā; ideju izvēršanu par to, kā uzlabot sadarbību starp ES un Austrumu partnerības valstīm, lai apkarotu kibernoziegumus; un pašreizējo problēmu apzināšanu, lai uzlabotu partnerības ar privāto sektoru.

Eiropas Kibernoziedzības apkarošanas apmācības un izglītības grupa (*ECTEG*)

Infotehnisko ekspertīžu nodaļas darbinieki (Valsts policijas Kriminālistikas pārvaldē) piedalījās *ECTEG* apmācībā (un nesen piedalījās apmācībā, kura tika sniegta sadarbībā ar Dublinas Universitātes koledžu un bija vērsta uz tādiem jautājumiem kā ļaunprogrammatūru analīze un izmeklēšana, kā arī ekspertīžu skriptēšana, izmantojot *bash* skriptu).

EIROPOLS/*EC3*

Valsts policijas darbinieki regulāri piedalās mācību pasākumos, ko nodrošina Eiropols/*EC3*. Piemēram, 2015. gadā Valsts policijas darbinieki piedalījās mācību pasākumos un ekspertu sanāksmēs, tostarp 16. Eiropola mācību kursā par bērnu seksuālas izmantošanas tiešsaistē apkarošanu, Eiropola ekspertu ikgadējā seminārā par bērnu seksuālu izmantošanu un interneta pedofīlijas apkarošanas projektā *(Fighting Internet Paedophilia Project – FIIP*).

Akadēmiskais sektors

Akadēmiskais sektors sniedz vērtīgu ieguldījumu, tādu kā, piemēram, visaptveroša kibernoziegumu izmeklēšanas rokasgrāmata, nozīmīga Satversmes tiesas veikta akadēmiskā analīze. Apmeklējuma laikā Valsts policijas koledža nebija izveidojusi sadarbību ar universitātes akadēmiķiem (piemēram, no Latvijas Universitātes vai Rīgas Tehniskās universitātes); tomēr pašlaik šī iespēja tiek pētīta.

Citas mācības

Valsts policijas darbinieki ir piedalījušies arī Māršala centra (*Marshall Centre*) nodrošinātajā apmācībā. 2014. gadā viens darbinieks piedalījās kibernoziedzības pētījumu programmas mācību kursā. 2015. gadā viens darbinieks piedalījās seminārā par kiberdrošību "Kiberdrošības apmācības absolventu interešu kopiena (semināra uzdevumi: praktiķu darbības)" (*Cyber alumni community of interest (workshop challenges: practitioner action)*) un divi darbinieki piedalījās kibernoziedzības pētījumu programmas mācību kursā.

Finansēšana

Mācību izmaksas sedz no vairākām Valsts policijas budžeta pozīcijām. Tāpēc nav iespējams aplēst Valsts policijas koledžas vai citu struktūru (tādu ka *CEPOL*) nodrošinātās regulārās apmācības moduļu /programmu kopējās gada izmaksas.

8.2. Informētības veicināšana

Latvijas prezidentūra ES Padomē *(2015. gada pirmā puse)*

Prezidentvalsts Latvija koncentrējās uz trim visaptverošām prioritātēm: *Konkurētspējīga Eiropa, Digitāla Eiropa* un *Iesaistīta Eiropa.*

Saistībā ar prioritāti *Digitāla Eiropa* prezidentvalsts Latvija organizēja vairākus pasākumus, kuri sekmēja gan informētības uzlabošanu, gan zināšanu apmaiņu, piemēram:

— *Digitālā asambleja 2015 – Viena Eiropa, viens digitālais vienotais tirgus* (2015. gada jūnijs), kas bija vērsta uz digitālā vienotā tirgus attīstību un tādiem jautājumiem kā uzticēšanās, piekļuves un savienojamības nodrošināšana, digitālās ekonomikas veidošana uzņēmumiem un patērētājiem un e-sabiedrības un digitālo prasmju veicināšana;

— *ES-28 mākoņdrošības konference* (sadarbībā ar *ENISA*; 2015. gada jūnijs), kas bija vērsta uz tādām tēmām kā juridiski un atbilstības jautājumi, tehnikas attīstība, privātuma un personas datu aizsardzība, kritiskās informācijas infrastruktūra un mākoņsertifikācija;

— *konference par informācijas un komunikācijas tehnoloģijām (IKT) informācijas pieejamībai mācībās* (2015. gada maijs), kuras uzmanības lokā bija tas, kā IKT izmantošana mācību procesā padara informāciju pieejamāku, tostarp cilvēkiem ar īpašām vajadzībām;

— *seminārs par kiberdrošības sistēmu* (2015. gada maijs), kurā tika izvērtētas dažādu ES dalībvalstu nacionālās stratēģijas un notika apmaiņa ar paraugpraksi (piemēram, par atbildīgu politiku incidentu atklāšanas jomā);

— *konference "E-prasmes nodarbinātībai 2015"* (2015. gada marts), kurā uzsvars tika likts uz digitālo prasmju apguvi un jaunu darbvietu izveidi nolūkā veicināt Eiropas ekonomisko izaugsmi (un tika arī pieņemta Rīgas deklarācija).

CERT.LV un Valsts policija

CERT.LV veicina informētību ne tikai par kibernoziegumiem, bet arī par plašākām tēmām, tādām kā drošība un privātums, un vairākiem konkrētiem jautājumiem (paroles, autentificēšana un citi) un īpašiem apdraudējumiem (pikšķerēšana, ļaunprogrammatūra, e-pasta pielikumi, identitātes zādzība). 2014. gadā CERT.LV bija iesaistīta 95 pasākumu organizēšanā ar gandrīz 6 000 dalībniekiem, un 2015. gadā – 104 pasākumu organizēšanā ar 6 680 dalībniekiem. Šajos pasākumos ir piedalījies plašs dalībnieku loks (sākot ar skolēniem līdz pat IT drošības speciālistiem un vadītājiem).

Valsts policijai ir aktīva *Facebook* lapa ar vairāk nekā 10 300 lietotājiem un *Twitter* konts ar 43 100 sekotājiem. Izmantojot šīs sociālo plašsaziņas līdzekļu platformas, regulāri tiek izplatīta informācija, kas saistīta ar kibernoziegumiem.

NVO ieguldījums informētības veicināšanā

Latvijas Informācijas un komunikācijas tehnoloģijas asociācija (LIKTA)
LIKTA tika nodibināta 1998. gadā, un tā apvieno vadošos nozares uzņēmumus un organizācijas, kā arī IKT jomas profesionāļus. LIKTA mērķis ir sekmēt Latvijas IKT nozares izaugsmi, veicinot informācijas sabiedrības un IKT izglītības attīstību, tādējādi uzlabojot Latvijas konkurētspēju pasaules mērogā.

LIKTA ietvaros ir arī izveidotas 11 darba grupas, tostarp izglītības/profesionālās izglītības attīstības darba grupa, datu aizsardzības un autortiesību darba grupa un darba grupa drošības un juridiskajos jautājumos digitālajā vidē. Turklāt LIKTA pasniedz gada balvu labākajam e-skolotājam. Novērtējot kandidātus, tiek izvērtēti šādi elementi: e-prasmju attīstība un informācijas sabiedrības (kā tādas) veicināšana; iekļautība (reģionālais aspekts un iesaistītās sociālās grupas); IKT izmantošanas un inovācijas (pieejas, metožu) veicināšana; IKT integrācija un e-prasmju attīstība izglītības procesā. 2015. gadā bija trīs finālisti; balva tika piešķirta skolotājam, kurš jau iepriekš arī bija iekļauts 500 vadošo inovatīvāko IT skolotāju sarakstā (*Microsoft* programmā "Partneri mācībās").

Latvijas Interneta asociācija (LIA)

Tā ir dibināta 2000. gadā; tās darbība ir vērsta uz interneta pieejamības veicināšanu Latvijā un tā izmantošanas stiprināšanu, pilnveidošanu un popularizēšanu. LIA ir Drošāka interneta centra *Net-Safe Latvia* koordinējošā struktūra, kuras uzmanības lokā galvenokārt ir bērnu izglītošana jautājumā par drošu un atbildīgu interneta lietošanu un ziņojumu līnijas darbības nodrošināšana, lai sabiedrībai būtu iespēja elektroniski ziņot par nelikumīgu tiešsaistes saturu un pārkāpumiem.

Digitālās drošības alianse (DDA)

DDA savu darbību sāka 2016. gada 9. februārī (Drošāka interneta dienas laikā), un tās mērķis ir veicināt informētību par interneta drošību (lietotājam saprotamā valodā), pievēršoties jo īpaši bērniem un jauniešiem (sociālajiem plašsaziņas līdzekļiem), un par e-banku un e-komercijas drošību.

Pasākumi

Kiberdrošības mēnesis (katrs oktobris)

Kiberdrošības mēneša laika tika organizēti vairāki pasākumi. Piemēram, 2015. gadā (CERT.LV sadarbībā ar vairākiem partneriem) organizēja konferenci "Kiberšahs. Stratēģija un taktika virtuālajā vidē". Tās uzmanības lokā bija tādi jautājumi kā drošība, stabilas un noturīgas identifikatoru sistēmas un kiberterorisms, un tā ietvēra vairākus seminārus.

Turklāt kopš 2012. gada CERT.LV katru gadu rīko akciju *Datorologs*, kuras laikā katram lietotājam ir iespēja bez maksas saņemt IT speciālistu sniegtu pakalpojumu – speciālisti pārbauda lietotāju personālos datorus, planšetdatorus vai viedtālruņus, lai tos "izārstētu" no vīrusiem, un konsultē par interneta drošību.

E-prasmju nedēļa (kopš 2012. gada)

Latvija aktīvi piedalās e-prasmju nedēļā; 2016. gadā kampaņas uzmanības lokā bija tādi jautājumi kā digitālās prasmes nodarbinātībai un nodarbināmībai, IKT drošība un datu aizsardzība. 2016. gadā e-prasmju nedēļa notika no 7. līdz 11. martam; nacionālie koordinatori ir LIKTA un Vides aizsardzības un reģionālās attīstības ministrija. Tika organizēti šādi galvenie pasākumi: pasākumi skolēniem un jauniešiem; skolotāju apmācība; digitālā diena uzņēmējiem un reģionālie semināri visā Latvijā.

Drošāka interneta diena

Katru gadu Drošāka interneta dienā Latvijā tiek organizētas vairākas informētības veicināšanas kampaņas un pasākumi. Piemēram, 2016. gada 9. februārī tika rīkots speciāls seminārs skolotājiem, kurš cita starpā ietvēra problēmjautājumus saistībā ar "tūkstošgades paaudzi" un jautājumu par attiecīgām mācību metodēm.

5. Izglītības un zinātnes ministrija

Izglītības un zinātnes ministrija īpašu uzmanību pievērš IKT zināšanu integrācijai izglītībā. Piemēram, pilotprojekts par e-prasmēm (programma "Datorika") ir īstenots 157 skolās; 2018./2019. gadā (pamatojoties uz pilotprojekta rezultātiem) pamatskolās tiks ieviests standarts par digitālajām prasmēm; tiek izstrādāti digitālie mācību materiāli un resursi; tiek izstrādāta jauna mācību programma atbilstoši jaunākajām IKT attīstības tendencēm, un tajā tiks iekļautas prasības par digitālajām prasmēm un plašsaziņas līdzekļu lietotprasmēm (tostarp e-drošību); studenti tiek mudināti izvēlēties karjeru IKT nozarē; un tiek uzlabotas skolotāju e-prasmes.

Izglītības un zinātnes ministrija un tai padotās iestādes ir izveidojušas ļoti labu sadarbību ar privāto sektoru, piemēram, ar LIKTA. 2016. gada februārī Valsts izglītības satura centrs noslēdza memorandu par sadarbību ar mērķi uzlabot IKT zināšanu integrāciju izglītībā un efektīvāk sasaistīt tās ar darba tirgu.

8.3. Prevencija

8.3.1. Valsts tiesību akti/politikas un citi pasākumi

Valsts policija izstrādā tīmekļa vietni www.sargi-sevi.lv, kas būs informācijas platforma drošības un prevencijas, tostarp kibernoziedzības, jautājumos. Bērni un jaunieši būs viena no mērķgrupām; katrai vecuma grupai tiks uzskaitīti un izskaidroti galvenie drošības apdraudējumi un bažas. Šo mērķi var sasniegt, iesaistot preventīvās darbībās bērnus un jauniešus kā instruktorus saviem vienaudžiem (apmācība vienaudžu līmenī). Izvērtētāji uzskata, ka tas varētu būt labs veids, kā ar ierobežotiem resursiem maksimāli palielināt preventīvo pasākumu efektivitāti.

Latvija augstu vērtē pastāvīgo reģionālo sadarbību starp Baltijas valstīm (ar Igauniju un Lietuvu). Piemēram, notiek aktīva pieredzes apmaiņa prevencijas jomā starp kompetentajām policijas iestādēm.

8.3.2. Publiskā un privātā partnerība (PPP)

Saskaņā ar Publiskās un privātās partnerības (PPP) likuma 1. pantu publiskā un privātā sektora partnerību vienlaikus raksturo šādas pazīmes:

- sadarbība notiek starp vienu vai vairākiem publiskajiem partneriem un vienu vai vairākiem publiskās un privātās partnerības procedūrā iesaistītajiem privātajiem partneriem;
- sadarbība notiek, lai nodrošinātu sabiedrības vajadzības būvdarbu veikšanā vai pakalpojumu sniegšanā;
- tā ir ilgtermiņa sadarbība, kas ilgst līdz 30 gadiem, bet šajā likumā paredzētajos gadījumos arī ilgāk;
- publiskais un privātais partneris apvieno un izmanto tam pieejamos resursus (piemēram, īpašumu, finanšu līdzekļus, zināšanas un pieredzi);
- atbildība un riski tiek dalīti starp publisko partneri un privāto partneri.

Latvija neizmanto publisko un privāto partnerību kibernoziedzības prevencijā un apkarošanā, kā definēts Publiskās un privātās partnerības likumā (gadījumos, kad ir paredzēta īpaša izpratne par PPP jēdzienu). Tomēr Valsts policija ir parakstījusi vienošanos par sadarbību ar CERT.LV un vienošanos par sadarbību ar Latvijas Interneta asociāciju (par nelikumīgu interneta saturu). Šajās vienošanās ir izklāstīti, piemēram, noteikumi par informācijas apmaiņu, zināšanu apmaiņu/apmācību un konkrētiem jautājumiem, tādiem kā piekļuves bloķēšana galalietotājiem vai nelikumīga interneta satura izņemšana.

8.4. Secinājumi

- Latvijas tiesnešu mācību centrs, NVO, ar kuru valdība ir noslēgusi ilgtermiņa vienošanos, lai nodrošinātu apmācību tiesu iestādēm, piedāvā tiesnešiem īsu neobligātu mācību kursu par kibernoziegumiem. Tas nodrošina tālākizglītību tiesnešiem un tiesu darbiniekiem. Šķiet, ka vajadzības gadījumā tas spēj organizēt un sniegt apmācību ieinteresētajiem tiesnešiem. Daži mācību kursi ir pieejami arī citiem praktizējošiem juristiem, piemēram, prokuroriem. Prokuratūra pauda uzskatu, ka esošās apmācības iespējas ir pietiekamas un nav nekādas vajadzības pēc kopīgām mācībām ar tiesnešiem vai policijas darbiniekiem kibernoziedzības jomā. Tomēr izvērtētāji novēroja, ka tiesnešiem un prokuroriem netiek sniegta pietiekama praktiska apmācība.

- No otras puses, Valsts policijas koledža piedāvā visaptverošu kibernoziedzības mācību programmu, kas aptver dažādus Valsts policijas personālam paredzētus moduļus. Šķiet, ka tā ir ļoti plaša un daudzveidīga un aptver visu jautājumu spektru, sākot ar kiberizmeklēšanas metodēm līdz labākajam elektronisku pierādījumu iegūšanas veidam. Tas liecina, ka papildus plašākai apmācībai, kas tiek sniegta specializētiem darbiniekiem, kuri strādā ar kibernoziedzības jautājumiem, aktīvajiem policijas darbiniekiem tiek nodots ievērojams zināšanu daudzums.

- Valsts policija jo īpaši atzinīgi vērtēja tematiskās sanāksmes un Eiropola un *Eurojust* sniegto apmācību kibernoziegumu izmeklēšanā un kriminālvajāšanā par tiem. Turklāt tiekoties praktiķi uzsvēra to, cik svarīgi ir dalīties pieredzē ES līmenī. Tie uzskatīja, ka īpaši svarīgi tas ir attiecībā uz kibernoziedzību, kas ir joma, kurā pieredze un risinājumi mainās ļoti ātri.

- Lai arī Valsts policijai ir ieviestas daudzas mācību iniciatīvas un dažas no tām ir paredzētas tiesu iestādēm, apmācība tiesnešiem, prokuroriem un Valsts policijai tiek nodrošināta atsevišķi. Kopīgas mācības starp visām iestādēm, kas iesaistītas kibernoziedzības gadījumu izmeklēšanā, kriminālvajāšanā par tiem un to izskatīšanā, varētu ievērojami veicināt procesa efektivitāti un ātrumu, kā arī palīdzēt apzināt vajadzīgās likumdošanas darbības vai izmaiņas praksē. Papildus tam, ka dalībniekiem tiek nodotas zināšanas, kopīgos mācību kursos var veidoties neformāls tīkls, kas apvieno par kibernoziedzības apkarošanu atbildīgās personas. Tas varētu palīdzēt labāk organizēt visu kibernoziedzības apkarošanas procesu un gūt labākus rezultātus visai valstij.

- Kas attiecas uz apmācību un prevenciju, izvērtētāji novēroja, ka sadarbība starp valsts pārvaldi un akadēmisko sektoru ir neliela. Izvērtētāji uzskata, ka šīs sadarbības veicināšana var palīdzēt stiprināt iestāžu spējas kibernoziedzības apkarošanā. Viens veids, kā to darīt, varētu būt tāds, ka tiek izveidots un atbalstīts daudzdisciplinārs Kiberaizsardzības izcilības centrs, kur akadēmiķi un vietējie eksperti no publiskā un privātā sektora var tikties, apmainīties ar pieredzi un zināšanām un tādējādi veicināt zinātniskās atziņas šajā jomā. Cits veids varētu būt mudināt akadēmiķus apsvērt izglītības programmu izstrādi kiberdrošības jomā, lai nodrošinātu pietiekamu kvalificētu profesionāļu pieplūdumu.

- Valsts policijas Kibernoziegumu apkarošanas nodaļa aktīvi sadarbojas ar nevalstiskajām organizācijām un privātā sektora projektiem, lai regulāri informētu neaizsargātās sociālās grupas, īpaši nepilngadīgos un pusaudžus, par riskiem internetā. Izvērtēšanas grupa tika arī informēta, ka Kibernoziegumu apkarošanas nodaļa atkarībā no saviem resursiem plāno izvērtēt, vai tai ir nepieciešams paplašināt savu darbības jomu, iekļaujot tajā arī citas neaizsargātās grupas, piemēram, vecāka gadagājuma cilvēkus. Tā kā savlaicīga prevencija lielā mērā palīdz samazināt sekmīgas kibernoziedzības gadījumu skaitu, īpaši attiecībā uz identitātes zādzību un pikšķerēšanu, šķiet, ka resursu ieguldīšana šajā jomā ir pārdomāts un slavējams pasākums, ar ko sekmēt cīņu pret kibernoziedzību. Tāpēc izvērtētāji uzskata, ka būtu lietderīgi izvērtēt, kuras citas neaizsargātās grupas bez nepilngadīgajiem un pusaudžiem varētu būt preventīvo pasākumu mērķgrupas, lai nodrošinātu pieejamo resursu optimālu izmantošanu un ieguldījumu visefektīvāko atdevi.

- CERT.LV organizē mācības reaģēšanai uz incidentiem, kuras paredzētas IT ekspertiem gan tehniskā līmenī, gan vadības līmenī.

- Dažādas publiskas struktūras Latvijā ir ieviesušas daudzus preventīvus pasākumus, tomēr tie netiek koordinēti. Pēc izvērtētāju domām, vienota kontaktpunkta norīkošana preventīvu darbību koordinēšanai starp ministrijām un ar citām attiecīgām struktūrām ļautu ietaupīt izmaksas un novērstu centienu dublēšanos. Preventīvos projektos būtu jāņem vērā citas iniciatīvas, jo dažas no tām attiecas uz tiem pašiem jautājumiem vai tām ir vienas un tās pašas mērķgrupas.

9. NOSLĒGUMA PIEZĪMES UN IETEIKUMI

9.1. Latvijas ierosinājumi

Latvijas iestādes uzskata, ka to vispārējās spējas ir pietiekamas. Apzinātās problēmas tiek risinātas. Latvija augstu vērtē reģionālo sadarbību ar savām Baltijas kaimiņvalstīm (Lietuvu un Igauniju) kibernoziedzības novēršanā un sadarbību starp to *CERT* vienībām. Turklāt sadarbība ar ASV valdību un lieliem ASV reģistrētiem uzņēmumiem arī tiek uzskatīta par svarīgu pasākumu kibernoziedzības apkarošanas pastiprināšanā. Ņemot vērā nozīmi, kāda tiek piešķirta kibernoziedzībai un kiberdrošībai ES iekšējās drošības stratēģijā 2015.–2020. gadam, Latvija cer, ka septītā izvērtējumu kārta dos papildu stimulu ES centieniem turpināt darbu pie apzinātajiem jautājumiem (konkrētāk, šifrēšana, elektroniskie pierādījumi, "mākoņa" jautājumi, jurisdikcijas jautājumi un datu glabāšana).

Latvijas iestādes arī minēja to, ka – tā kā Saeima interesējas par Nacionālās IT drošības padomes darbu – ar likumdošanas palīdzību tiek nodrošināta ātra reaģēšana uz praksē apzinātajām problēmām un uzdevumiem.

9.2. Ieteikumi

Kas attiecas uz Pamatlēmuma un direktīvu praktisko īstenošanu un darbību, izvērtējumā iesaistītā ekspertu grupa spēja apmierinoši pārskatīt sistēmu Latvijā.

Latvijai 18 mēnešu laikā pēc izvērtēšanas būtu jāveic pēcpasākumi saistībā ar šajā ziņojumā minētajiem ieteikumiem un jāziņo par progresu Vispārējo lietu, tostarp izvērtējumu, darba grupai (*GENVAL*).

Izvērtēšanas grupa uzskatīja par lietderīgu sniegt Latvijas iestādēm vairākus ierosinājumus. Turklāt, pamatojoties uz dažādām labām praksēm, ir sniegti arī saistītie ieteikumi ES un tās iestādēm un aģentūrām, jo īpaši Eiropolam.

9.2.1. Ieteikumi Latvijai

1. Būtu jāapsver iespēja Prokuratūrā vairāk specializēties kibernoziedzības jautājumos (sk. 4.1.1. un 4.5. sadaļu).

2. Būtu vēl vairāk jāizmanto esošās struktūras un kanāli, lai uzlabotu koordināciju starp kiberdrošībā iesaistītajiem dalībniekiem, jo īpaši optimālāk izmantojot Nacionālās IT drošības padomes spējas un autoritatīvo stāvokli (sk. 4.4.1. un 4.5. sadaļu).

3. Būtu jāapsver iespēja konkrētos koordinācijas projektos Nacionālās IT drošības padomes struktūras ietvaros – piemēram, prevencijas jomā – iesaistīt konkrētus privātā sektora partnerus, lai novērstu trūkumus vai pārklāšanos kibernoziedzības apkarošanā (sk. 4.2., 4.5. un 6.4. sadaļu).

4. Būtu jāmudina Valsts policijas līmenī izveidot vienu struktūrvienību, kas atbildētu par kibernoziedzības jautājumiem, lai atbalstītu un koordinētu visu policijas struktūrvienību centienus un veiktu pienācīgu izmeklēšanu, īpaši smagākajos kibernoziedzības gadījumos (sk. 4.2. un 4.5. sadaļu).

5. Būtu jāmudina pastāvīgi likt uzsvaru uz mērķorientētu resursu uzturēšanu un palielināšanu, lai stiprinātu valsts spēju kibernoziedzības apkarošanā, īpaši Valsts policijas centrālajā un reģionālajā līmenī (sk. 4.4.2. un 4.5. sadaļu).

6. Būtu tālāk jāizstrādā pamatnostādnes par to, kā piemērot esošos noteikumus par kompetenču sadalījumu naida noziegumu izmeklēšanā (sk. 3.5. un 5.5. sadaļu).

7. Būtu jāapsver iespēja uzlabot procedūras digitālo datu izņemšanai, ieviešot spoguļkopēšanu kā standartprocedūru, lai iedrošinātu cilvēkus labprātāk sadarboties ar tiesībaizsardzības iestādēm (sk. 5.2.1. un 5.5. sadaļu).

8. Būtu jāapsver iespēja paplašināt preventīvās darbībās, attiecinot tās arī uz citām neaizsargātām grupām, kas nav nepilngadīgie, un norīkot vienotu kontaktpunktu preventīvu darbību koordinēšanai ar citiem attiecīgiem dalībniekiem, tādiem kā NVO (sk. 6.2.3. un 6.4. sadaļu).

9. Būtu jāapsver iespēja uzlabot attiecības starp valsts pārvaldi un akadēmisko sektoru, lai stiprinātu tās spējas kibernoziedzības apkarošanā (sk. 6.4., 8.1. un 8.4. sadaļu).

10. Būtu jāturpina organizēt praktisko apmācību tiesnešiem un prokuroriem, lai uzlabotu viņu speciālo zināšanu līmeni, un jāapsver iespējas izstrādāt kopīgu mācību/pieredzes apmaiņas koncepciju, kas ietver visas kibernoziedzības apkarošanā iesaistītās grupas (prokurorus, tiesnešus un policijas darbiniekus) (sk. 8.1. un 8.4. sadaļu).

9.2.2. Ieteikumi Eiropas Savienībai, tās iestādēm un citām dalībvalstīm

1. Dalībvalstīm iesaka pilnībā izmantot pieejamos civilos resursus, lai uzlabotu savas kiberaizsardzības spējas gan miera laikā, gan krīzes situācijās, kā to dara Latvija, izmantojot Kiberaizsardzības vienību (sk. 6.1.2. un 6.4. sadaļu).

2. Dalībvalstīm iesaka izveidot ciešas attiecības starp kiberdrošībā iesaistītajiem dalībniekiem, kuri pārstāv dažādas specializācijas un profilus un kuru uzdevums ir kalpot sabiedrībai kopumā, tādiem kā, piemēram, CERT.LV Latvijā (sk. 4.3., 4.5., 6.1.2. un 6.4. sadaļu).

3. Dalībvalstīm iesaka izmantot instrumentus, lai apkarotu vardarbību pret bērniem un bērnu pornogrāfiju tiešsaistē, izstrādājot instrumentus, kas ļauj ziņot par nelikumīgu saturu internetā, tādus kā, piemēram, Drošāka interneta centra *Net-Safe Latvia* projekts (sk. 6.2.3. un 6.5. sadaļu).

4. Dalībvalstīm iesaka strādāt pie risinājumiem, lai uzlabotu un paātrinātu ar kibernoziedzību saistīto savstarpējās tiesiskās palīdzības lūgumu izpildi (sk. 7.3. un 7.6. sadaļu).

5. ES iestādēm būtu jārisina jautājums par datu glabāšanu (sk. 5.2.1. un 5.5. sadaļu).

6. ES būtu jāapsver iespēja koordinēt centienus noteikt efektīvu veidu, kā paziņot par savstarpējas tiesiskās palīdzības lūgumiem, ko ES dalībvalstis nosūta trešām valstīm, un kā izpildīt šādus lūgumus, vai izveidot sistēmu tiešai sadarbībai ar attiecīgajiem ārpussavienības interneta pakalpojumu sniedzējiem (sk. 7.6. sadaļu).

9.2.3. Ieteikumi Eurojust/*Eiropolam*/ENISA

1. *Eurojust* un Eiropols tiek aicināti izveidot platformu, kas visiem attiecīgajiem kibernoziedzības apkarošanā iesaistītajiem dalībniekiem darītu pieejamu visu informāciju, kas nepieciešama, lai iesniegtu savstarpējas tiesiskās palīdzības lūgumu citām ES dalībvalstīm vai kaimiņvalstīm (sk. 7.6. sadaļu).

2. *Eurojust*/Eiropas Tiesiskās sadarbības tīkls (*EJN*) tiek aicināti pielikt pūles, lai izveidotu forumu, kur varētu regulāri apmainīties ar pieredzi attiecībā uz kriminālvajāšanu par kibernoziegumiem un attiecībā uz tiesu iestāžu sadarbības instrumentu izmantošanu, kā arī formālajām prasībām, kas tiem paredzētas (sk. 7.6. sadaļu).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

MINISTRYOFTHEINTERIOROFTHEREPUBLICOF

LATVIA

7TH ROUND OF MUTUAL EVALUATIONS

The practical implementation and operation of EU policies on preventing and combating cybercrime

VISIT TO LATVIA

7 – 11 March 2016

Monday 7 March

	Arrival	
19.30	Informal meeting *Radisson Blu Rīdzene Hotel* *Reimersa iela 1*	Representatives from the Ministry of the Interior (MoI)

Tuesday 8 March

10.00 – 10.30	Opening by the MoI *Čiekurkalna 1. līnija 1, k. 2*	*Mr Dimitrijs Trofimovs,* Deputy State Secretary, MoI Representatives from the MoI and the State Police

10.30 – 12.30	Meeting with the State Police *Čiekurkalna 1. līnija 1, k. 2*	*Mr Gatis Švika,* Head, Cooperation and Development Bureau, Central Administrative Department, State Police *Ms Brigita Lasenberga,* Deputy Head, Criminal Intelligence Department, Central Criminal Police Department, State Police *Mr Andis Rinkevics*, Head, Crime Prevention Unit, Central Public Order Police Department, State Police *Ms Dina Tarāne*, Deputy Director,
		State Police College *Mr Aleksandrs Bebris*, Lecturer, State Police College
12.30 – 13.30	Lunch provided by the MoI and the State Police *Čiekurkalna 1. līnija 1, k. 2*	

13.30 – 16.00	Meeting with the State Police *Čiekurkalna 1. līnija 1, k. 2*	*Ms Aleksandra Tukiša,* Head, Operational Coordination and Information Provision Unit, International Cooperation Bureau, Central Criminal Police Department, State Police *Mr Deniss Belouss,* Acting Head, Forensic IT Unit, Forensics Department, State Police Economic Crime Enforcement Department, State Police: Unit 4: – *Mr Dmitrijs Homenko,* Head – *Mr Jānis Tikums,* Senior Inspector – *Mr Aleksandrs Bebris*, Senior Inspector – *Mr Dzintars Vikšers,* Senior Inspector Unit 1: – *Ms Inese Gise*, Head – *Mr Jānis Barens,* Senior Inspector
18.00	Dinner provided by the Deputy State Secretary, MoI *'Kolonāde' restaurant, Brīvības bulvāris 26*	

Wednesday 9 March

10.00 – 12.00	Meeting at the Ministry of Defence (MoD) and CERT.LV *Kr. Valdemāra iela 10/12*	*Mr Einārs Leps,* Senior Expert, National Cybersecurity Policy Coordination Section, MoD *Mr Edgars Tauriņš,* IT Security Expert, CERT.LV
12.30 – 13.30	Lunch provided by the MoD *'Amarone' restaurant, Jura Alunāna iela 2*	
14.00 – 15.00	Meeting with the *Net-safe Latvia* Safer Internet Centre *Brīvības gatve 214M – 206*	*Ms Maija Katkovska,* Director *Ms Anita Ērgle*, Expert, Family Support Department, the State Inspectorate for Protection of Children's Rights *Ms Anda Sauļūna*, Expert, Family Support Department, the State Inspectorate for Protection of Children's Rights
15.30 – 16.30	Meeting with the Latvian Information and Communication Technology Association *Stabu iela 47*	*Mr Andris Melnūdris*, Director

Thursday 10 March

9.30 – 12.00	Meeting at the Ministry of Justice (MoJ) *Brīvības bulvāris 36*	*Ms Ilze Vanaga*, Judge, City of Riga Zemgale Urban District Court *Ms Kristīne Pommere*, Director, Department of European Affairs, MoJ *Mr Uldis Zemzars,* Legal Adviser, Department of Criminal Law, MoJ *Ms Elīna Feldmane,* Legal Adviser, Department of Criminal Law, MoJ *Mr Viktors Makucevičs*, Legal Adviser, Department of Judicial Cooperation, MoJ *Ms Dārta Mestere,* Legal Programme Officer, Latvian Judicial Training Centre
12.30 – 13.30	Lunch on behalf of the Prosecutor's General Office (PGO) *Radisson Blu Hotel Latvija* *Elizabetes iela 55*	

14.00 – 16.00	Meeting at the PGO *Kalpaka bulvāris 6*	*Ms Una Brenča*, Head Prosecutor, International Cooperation Division, PGO *Ms Dagmāra Skudra*, Prosecutor, International Cooperation Division, PGO *Mr Mārcis Viļums,* Prosecutor, International Cooperation Division, PGO *Mr Gatis Doniks*, Prosecutor, Methodology Division, PGO *Mr Ingemārs Masaļskis*, Head Prosecutor, Specially Authorised Prosecutors' Division, PGO *Mr Kaspars Cakuls*, Prosecutor, Prosecution Office of Riga Judicial Region *Mr Mairis Mackēvičs*, Prosecutor, Prosecution Office of Riga Judicial Region

Friday 11 March

9.30 – 10.00	Meeting with the Digital Security Alliance *Čiekurkalna 1. līnija 1, k. 2*	*Ms Sanita Igaune,* Director Representative from *Swedbank*
10.00 – 12.00	Overview of the evaluation visit (wrap-up session) *Čiekurkalna 1. līnija 1, k. 2* Departure	Representatives from the MoI and the State Police

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 8 March 2016

Venue: Ministry of the Interior

Person interviewed/met	Organisation represented
Mr Dimitrijs Trofimovs	Deputy State Secretary Ministry of the Interior
Ms Anete Valaine-Elsone	Legal Adviser, Ministry of the Interior
Ms Asnāte Kalniņa	Legal Adviser, Ministry of the Interior
Mr Gatis Švika	Head, Cooperation and Development Bureau, Central Administrative Department of the State Police
Ms Brigita Lasenberga	Deputy Head, Criminal Intelligence Department, Central Criminal Police Department of the State Police
Mr Andis Rinkevics	Head, Crime Prevention Unit, Central Public Order Police Department
Ms Dina Tarāne	Deputy Director, State Police College
Mr Aleksandrs Bebris	Lecturer, State Police College Senior Inspector, Group 2, Unit 4, Economic Crime Enforcement Department
Ms Aleksandra Tukiša	Head, Operational Coordination and Informative Provision Unit, International Cooperation Bureau, Central Criminal Police Department
Ms Olga Trocka	Head, Legal Assistance Request Unit, International Cooperation Bureau, Central Criminal Police Department
Mr Deniss Belouss	Acting Head, Forensic IT Unit, Forensics Department
Mr Dmitrijs Homenko	Head, Unit 4, Economic Crime Enforcement Department

Mr Jānis Tikums	Senior Inspector, Group 1, Unit 4, Economic Crime Enforcement Department
Mr Dzintars Vikšers	Senior Inspector, Group 3, Unit 4, Economic Crime Enforcement Department
Ms Inese Gise	Head, Unit 1, Economic Crime Enforcement Department
Mr Jānis Barens	Senior Inspector, Unit 1, Economic Crime Enforcement Department

Meetings on 9 March 2016

Venue: Ministry of Defence

Person interviewed/met	**Organisation represented**
Ms Ieva Ilves	Head, National Cyber Security Policy Coordination Section
Mr Einārs Leps	Senior Expert, National Cyber Security Policy Coordination Section
Ms Elīna Neimane	Senior Desk Officer, National Cyber Security Policy Coordination Section
Mr Ēriks Dobelis	Member of the Cyber Defence Unit National Guard
Mr Edgars Tauriņš	IT Security Expert, CERT.LV

Venue: Net-Safe Latvia Safer Internet Centre

Person interviewed/met	**Organisation represented**
Ms Maija Katkovska	Director
Ms Anita Ērgle	Expert, Family Support Department
Ms Anda Sauļūna	Expert, Family Support Department

Venue: Latvian Information and Communication Technology Association (LIKTA)

Person interviewed/met	Organisation represented
Ms Māra Jākobsone	Vice President
Mr Andris Melnūdris	Managing Director
Mr Toms Pēcis	IT risk manager, Lattelecom

Meetings on 10 March 2016

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Ms Ilze Vanaga	Judge, City of Riga Zemgale Urban District Court
Mr Uldis Zemzars	Legal Adviser, Department of Criminal Law, Ministry of Justice
Ms Elīna Feldmane	Legal Adviser, Department of Criminal Law, Ministry of Justice
Mr Viktors Makucevičs	Legal Adviser, Department of Judicial Cooperation, Ministry of Justice
Ms Dārta Mestere	Legal Programme Officer

Venue: Prosecutor-General's Office

Person interviewed/met	Organisation represented
Ms Una Brenča	Head Prosecutor, International Cooperation Division, Prosecutor-General's Office
Ms Dagmāra Skudra	Prosecutor, International Cooperation Division, Prosecutor-General's Office
Mr Gatis Doniks	Prosecutor, Methodology Division, Prosecutor-General's Office
Mr Ingemārs Masaļskis	Head Prosecutor, Specially Authorised Prosecutors' Division, Prosecutor-General's Office

Person interviewed/met	Organisation represented
Mr Kaspars Cakuls	Prosecution Office of Riga Judicial Region

Venue: CERT.LV

Person interviewed/met	Organisation represented
Ms Baiba Kaškina	Director
Mr Varis Teivāns	Deputy Director
Mr Edgars Tauriņš	IT Security Expert

Meetings on 11 March 2016

Venue: Ministry of the Interior

Person interviewed/met	Organisation represented
Ms Sanita Igaune	Director, Digital Security Alliance
Mr Vitālijs Kuzmins	IT risk manager, Swedbank
Name and surname not to be disclosed	Security Police
Mr Gatis Švika	Head, Cooperation and Development Bureau, Central Administrative Department
Ms Brigita Lasenberga	Deputy Head, Criminal Intelligence Department, Central Criminal Police Department
Ms Inga Šamarova	Head, Information Bureau, Central Criminal Police Department
Mr Jānis Kruks	IT security administrator
Ms Aleksandra Tukiša	Head, Operational Coordination and Information Provision Unit, International Cooperation Bureau, Central Criminal Police Department

Person interviewed/met	Organisation represented
Mr Deniss Belouss	Acting Head, Forensic IT Unit, Forensics Department
Mr Dmitrijs Homenko	Head, Unit 4, Economic Crime Enforcement Department
Mr Jānis Tikums	Senior Inspector, Group 1, Unit 4, Economic Crime Enforcement Department
Mr Dzintars Vikšers	Senior Inspector, Group 3, Unit 4, Economic Crime Enforcement Department
Mr Mārtiņš Brižs	Senior Inspector, Unit 4, Economic Crime Enforcement Department
Ms Inese Gise	Head, Unit 1, Economic Crime Enforcement Department

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	**LATVIAN OR ACRONYM IN ORIGINAL LANGUAGE**	**LATVIAN OR ACRONYM IN ORIGINAL LANGUAGE**	**ENGLISH**
BDPS	*BDPS*		Biometric Data Processing System
CEU	*CEU*		Cybercrime Enforcement Unit
CPU	*CPU*		Crime Prevention Unit
CSS	*CSS*		Cyber Security Strategy of Latvia 2014-2018
DDA	*DDA*		Digital Safety Alliance
DSI	*DSI*		Data State Inspectorate
HAVEN	*HAVEN*		Halting Europeans Abusing Victims in Every Nation
IIIS	*IIIS*		Integrated Interior Information System
KRASS	*KRASS*		Criminal Procedure Information System
LIA	*LIA*		Latvian Internet Association
LIKTA	*LIKTA*		Latvian Information and Communication Technology Association
OCIPU	*OCIPU*		Operational Coordination and Information Provision Unit
TIS	*TIS*		Court Information System

Under the **Criminal Law**, the following acts are criminalised:

1) violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (namely, illegal interception; Article 144):

— for *intentional violation of the confidentiality of personal correspondence*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 144(1));

— for *unlawful interception of publicly unavailable data transmissions or signals in telecommunications networks, as well as unlawful acquisition of publicly unavailable electromagnetic data from a telecommunications network in which such data is present*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 144(2));

— if the acts provided for in Article 144(1) or (2) are committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine (Article 144(3));

2) obtaining, manufacture, distribution, utilisation and storage of data, software and equipment for illegal acts with financial instruments and means of payment (Article 193^1):

— for *obtaining or distribution of such data as enable illegal utilisation of financial instruments or means of payment*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 193^1(1));

— for *utilisation of such data as enable illegal utilisation of financial instruments or means of payment, or manufacture or adaptation of software or equipment for the commission of the crimes provided for in Article 193 of the Criminal Law, or obtaining, storage or distribution of such software or equipment for the same purpose*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 193^1(2));

— if the acts provided for in Article 193^1(1) or (2) *are committed by a member of an organised group*, the applicable punishment is deprivation of liberty for a term of between two and ten years, with or without confiscation of property and with police supervision for a term of up to three years (Article 193^1(3));

3) the arbitrary accessing of automated data processing systems (Article 241):

— for *arbitrary accessing of an automated data processing system, if it is related to a breach of system protective measures or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 241(1));

— for the criminal offence provided for in Article 241(1), if it has been committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to four years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 241(2));

— for the acts provided for in Article 241(1), *if serious consequences have been caused thereby, or if they are directed against automated data processing systems that process information related to state political, economic, military, social or other security*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property (Article 241(3));

4) interference in the operation of automated data processing systems and illegal actions with the information included in such systems (Article 243):

— for *unauthorised modification, damage, destruction, impairment or concealment of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 243(1));

— for *knowingly interfering in the operation of an automated data processing system by entering, transferring, damaging, erasing, impairing, changing or hiding information, if the protective system is damaged or destroyed thereby and substantial harm is caused*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine (Article 243(2));

— for the criminal offence provided for in Article 243(1) or (2), if it has been committed *for the purposes of acquiring property*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with or without police supervision for a term of up to three years (Article 243(3));

— for the acts provided for in Article 243(1) or (2), *if they have been committed by an organised group or if they have caused serious consequences, or if they are directed against an automated data processing system that processes information related to state political, economic, military, social or other security*, the applicable punishment is deprivation of liberty for a term of up to seven years, with or without confiscation of property and with or without probationary supervision for a term of up to three years (Article 243(5));

5) illegal operations with devices influencing automated data processing system resources (Article 244):

— for *illegal manufacture, adaptation for utilisation, sale, distribution or storage of a tool (device, software, computer password, access code or similar data) intended to influence the resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for the purposes of committing a criminal offence*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine (Article 244(1));

— for the same acts, *if serious consequences have been caused thereby*, the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine (Article 244(2));

6) acquisition, development, alteration, storage and distribution of data, programs and equipment for illegal activities with electronic communications network terminal equipment (Article 244):

— for *electronic communications network terminal equipment identification in an electronic communications network for necessary data alterations or the acquisition, storage or distribution of data intended for such purposes, as well as the acquisition, development, storage or distribution of programs or equipment intended for such purposes, without the consent of the manufacturer or the authorised person thereof,* if such activities have been committed for the purposes of acquiring property or if it has been committed by a group of persons pursuant to prior agreement, or if it has caused *significant harm*, the applicable punishment is either deprivation of liberty for a term of up to two years, temporary deprivation of liberty, community service or a fine.

Content-related acts, in particular those related to child sexual abuse

1) encouraging participation in sexual acts (Article 162[1]):

— for *encouraging, using information or communication technologies or other means of communication, a person who has not attained the age of sixteen to participate in sexual acts or to meet with the aim of committing sexual acts or entering into a sexual relationship, if such act has been committed by a person who has attained the age of majority*, the applicable punishment is either deprivation of liberty for a term of up to four years, temporary deprivation of liberty, community service or a fine, with probationary supervision for a term of up to five years (Article 162[1](1));

— if the acts provided for in Article 162[1](1) are *committed against an underage person,* the applicable punishment is either deprivation of liberty for a term of up to five years, temporary deprivation of liberty, community service or a fine, with probationary supervision for a term of up to five years (Article 162[1](2));

2) violation of provisions regarding the demonstration of a pornographic performance, the restriction of entertainment of an intimate nature and the handling of material of a pornographic nature (Article 166):

— for *violation of provisions regarding the demonstration of a pornographic performance, provisions regarding the restriction of entertainment of an intimate nature, or provisions regarding the handling of material of a pornographic nature, if substantial harm has been caused by the commission thereof*, the applicable punishment is either deprivation of liberty for a term of up to one year, temporary deprivation of liberty, community service or a fine (Article 166(1));

— for *visiting or demonstrating such pornographic performance or handling materials of a pornographic nature which contain child pornography, sexual activities of people with animals, necrophilia or sexual gratification in a violent way*, the applicable punishment is either deprivation of liberty for a term of up to three years, temporary deprivation of liberty, community service or a fine, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(2));

— for *involvement, forced participation or utilisation of minors in a pornographic performance or the production of material of a pornographic nature, or for encouraging their participation therein*, the applicable punishment is deprivation of liberty for a term of up to six years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(3));

— for *involvement, forced participation or utilisation of persons who have not attained the age of sixteen in a pornographic performance or the production of material of a pornographic nature, or for encouraging their participation therein*, the applicable punishment is deprivation of liberty for between three and twelve years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(4));

— if the acts provided for in Article 166(3) or (4) are committed by *an organised group or if they have been committed by means of violence*, the applicable punishment is deprivation of liberty for a term of between five and fifteen years, with or without confiscation of property and with probationary supervision for a term of up to three years (Article 166(5)).

Intent/recklessness

Article 8 of the Criminal Law (on forms of guilt) states that 'only a person who has committed a criminal offence *deliberately (intentionally)* or through *negligence* may be found guilty of it', and further explains that 'in determining the form of guilt of a person who has committed a criminal offence, the mental state of the person in relation to the objective elements of the criminal offence must be established'.

According to Article 9, 'a criminal offence shall be considered to have been committed *deliberately (intentionally)* if the person has committed it with *direct or indirect intent*'. It further explains that a criminal offence is considered to have been committed with:

— *direct intent* if the person has been aware of the harm caused by his or her act or failure to act and has knowingly committed it, or has been aware of the harm caused by his or her act or failure to act, has foreseen the harmful consequences of the offence and has desired them.

— *indirect intent* if the person has been aware of the harm caused by his or her act or failure to act, has foreseen the harmful consequences of the offence and, although not desiring such consequences, has knowingly allowed them to result.

According to Article 10, 'a criminal offence shall be considered to be committed through *negligence* if the person has committed it through *criminal self-reliance or criminal neglect*'. It is further explained that a criminal offence is considered to have been committed through:

— *criminal self-reliance* if the person has foreseen the possibility that the harmful consequences of his or her act or failure to act would result and nevertheless carelessly relied on their being prevented;

— *criminal neglect* if the person did not foresee the possibility that the consequences of his or her act or failure to act would result, even though according to the actual circumstances of the offence he or she should and could have foreseen such harmful consequences.

Aggravating/mitigating factors

According to Article 46 of the Criminal Law on general principles for determination of punishment, in determining the amount of punishment, the circumstances *mitigating or aggravating* the liability must be taken into account.

Article 47 sets out the following circumstances which are to be considered as *mitigating* the liability:

— if the perpetrator of the criminal offence has admitted his or her guilt, has freely confessed and has regretted the criminal offence committed;

— if the offender has:

- actively furthered the disclosure and investigation of the criminal offence;
- voluntarily compensated the harm caused by the criminal offence to the victim or has eliminated the harm caused;
- facilitated the disclosure of a crime of another person;

  — if the criminal offence was committed:
- as a result of unlawful or immoral behaviour by the victim;
- exceeding the conditions regarding necessary self-defence, extreme necessity, detention of the person committing the criminal offence, justifiable professional risk, or the legality of the execution of a command or order;
- by a person in a state of diminished mental capacity.

However, other circumstances which are related to the criminal offence committed may also be considered as mitigating the liability.

According to Article 48, the following may be considered to be *aggravating* circumstances:

— if the criminal offence was committed:

- while in a group of persons;
- by taking advantage, in bad faith, of an official position or the trust of another person;
- against a woman, knowing her to be pregnant;
- against a person who has not attained sixteen years of age or by taking advantage of the helpless condition or infirmity due to old age of a person;
- by taking advantage of a person's official, financial or other dependence on the offender;
- with particular cruelty or with humiliation of the victim;
- by taking advantage of the circumstances of a public disaster;
- using weapons or explosives, or in some other generally dangerous way;
- out of a desire to acquire property;
- under the influence of alcohol or of narcotic, psychotropic, toxic or other intoxicating substances;
- for racist, national, ethnic or religious motives;

  — if the criminal offence:

- has caused serious consequences;
- constitutes *recidivism* of criminal offences;
- was related to violence or threats of violence, or if the criminal offence against morality and sexual inviolability was committed against a person to whom the perpetrator is related in the first or second degree of kinship, against the spouse or former spouse, against a person with whom the perpetrator is or has been in an unregistered marital relationship, or against a person with whom the perpetrator has a joint (single) household;

- if the person committing the criminal offence, for the purposes of having his or her punishment reduced, has knowingly provided false information regarding a criminal offence committed by another person.

Multiple crimes/recidivism

According to Article 24, multiplicity of criminal offences is 'the commission (or allowing) by one person of two or more separate offences (act or failure to act) which correspond to the constituent elements of several criminal offences, or the commission (or allowing) by a person of one offence (act or failure to act) which corresponds to the constituent elements of at least two different criminal offences'. It is further explained that 'multiplicity of criminal offences is constituted by aggregation and *recidivism* of criminal offences'.

Article 27 explains that '*recidivism* of a criminal offence is constituted by a new intentional criminal offence committed by a person after the conviction of such person for an intentional criminal offence committed earlier, if the criminal record for such has not been set aside or extinguished in accordance with the procedures laid down in law'.

Incitement, aiding and abetting

Article 19 on participation states that 'criminal acts committed knowingly by which two or more persons (that is, a group) jointly, knowing such, have directly committed an intentional criminal offence shall be considered to be participation (*joint commission*)' and that 'each of such persons is a participant (joint perpetrator) in the criminal offence'.

According to Article 20 on joint participation, 'an act or failure to act committed knowingly, by which a person (joint participant) has jointly with another person (perpetrator), participated in the commission of an intentional criminal offence, but he himself or she herself has not been the direct perpetrator of it, shall be considered to be joint participation' and that '*organisers, instigators and abettors* are joint participants in a criminal offence'.

Attempt

According to Article 15 on completed and uncompleted criminal offences, 'a conscious act (failure to act), which is directly dedicated to the intentional commission of a crime, shall be considered to be an *attempted* crime if the crime has not been completed for reasons independent of the will of the guilty party'.

'Serious' or 'large-scale' cyber-attack

According to Article 20 of *On the Procedures for the Coming into Force and Application of the Criminal Law*, 'liability for an offence provided for in the Criminal Law which has been committed on a **large scale** shall apply if the total value of the property which was the subject of the offence was not less than fifty times the minimum monthly wage as specified in the Republic of Latvia at that time'. The Article further explains that 'the value of the property shall be determined according to the market prices or prices equivalent thereto at the time when the offence was committed'.

As regards the notion of **substantial harm**, Article 23 clarifies that "liability for the criminal offence provided for in the Criminal Law, by which substantial harm has been caused, shall apply, if one of the following consequences has been caused:

— financial loss which at the time of committing the crime has not been less than five times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia, *and* if other interests protected by law have been threatened;

— financial loss which at the time of committing the crime has not been less than ten times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia;

— other interests protected by law have been significantly threatened.

Article 24 specifies that "liability for a criminal offence provided for in the Criminal Law that has caused **serious consequences** shall apply if the criminal offence has resulted in death of a person, or serious bodily injuries or psychological trauma to at least one person, moderate bodily harm to a number of persons or financial loss, which at the time of committing the crime has not been less than fifty times the minimum monthly wage (in total) as determined at the time in the Republic of Latvia, have been inflicted, or other serious harm has been caused to the interests protected by law.[17]

[17] The criteria for the specification of the level of seriousness of bodily injury are provided for in annexes to this Law.